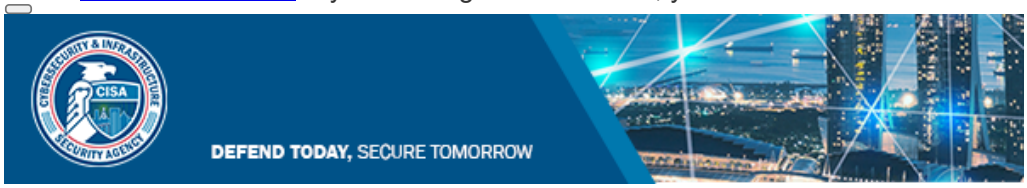

Vulnerability Summary for the Week of April 26, 2021

Cybersecurity and Infrastructure Security Agency sent this bulletin at 05/03/2021 01:32 PM EDT

You are subscribed to National Cyber Awareness System Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

Vulnerability Summary for the Week of April 26, 2021

05/03/2021 08:20 AM EDT

Original release date: May 3, 2021

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
avaya -- session_border_controller_for_enterprise	A command injection vulnerability in Avaya Session Border Controller for Enterprise could allow an authenticated, remote attacker to send specially crafted messages and execute arbitrary commands with the affected system privileges. Affected versions of Avaya Session Border Controller for Enterprise include 7.x, 8.0 through 8.1.1.x	2021-04-23	9	CVE-2020-7034 CONFIRM
ibm -- spectrum_protect_backup-archive_client	IBM Spectrum Protect Client 8.1.0.0 through 8.1.11.0 could allow a local user to escalate their privileges to take full control of the system due to insecure directory permissions. IBM X-Force ID: 198811.	2021-04-26	7.2	CVE-2021-20532 CONFIRM XF
ibm -- spectrum_protect_client	IBM Spectrum Protect Client 8.1.0.0-8 through 1.11.0 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking when processing the current locale settings. A local attacker could overflow a buffer and execute arbitrary code on the system with elevated privileges or cause the application to crash. IBM X-Force ID: 199479	2021-04-26	7.2	CVE-2021-29672 CONFIRM XF
inxedu -- inxedu	SQL Injection in com/inxedu/OS/edu/controller/letter/AdminMsgSystemController in Inxedu v2.0.6 via the ids parameter to admin/letter/delsystem.	2021-04-29	7.5	CVE-2020-35430 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jquery-bbq_project -- jquery-bbq	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-bbq 1.2.1 allows a malicious user to inject properties into Object.prototype.	2021-04-23	7.5	CVE-2021-20086 MISC
manta -- safe-obj	Prototype pollution vulnerability in 'safe-obj' versions 1.0.0 through 1.0.2 allows an attacker to cause a denial of service and may lead to remote code execution.	2021-04-26	7.5	CVE-2021-25928 MISC MISC
nec -- aterm_wg2600hs_firmware	Aterm WG2600HS firmware Ver1.5.1 and earlier allows an attacker to execute arbitrary OS commands via unspecified vectors.	2021-04-26	10	CVE-2021-20711 MISC MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an integer overflow in the regional allocator via regional_alloc.	2021-04-27	7.5	CVE-2019-25032 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an integer overflow in the regional allocator via the ALIGN_UP macro.	2021-04-27	7.5	CVE-2019-25033 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an integer overflow in sldns_str2wire_dname_buf_origin, leading to an out-of-bounds write.	2021-04-27	7.5	CVE-2019-25034 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an out-of-bounds write in sldns_bget_token_par.	2021-04-27	7.5	CVE-2019-25035 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an integer overflow in a size calculation in dnscrypt/dnscrypt.c.	2021-04-27	7.5	CVE-2019-25038 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an integer overflow in a size calculation in respip/respip.c.	2021-04-27	7.5	CVE-2019-25039 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an out-of-bounds write via a compressed name in rdata_copy.	2021-04-27	7.5	CVE-2019-25042 MISC
pulsesecure -- pulse_connect_secure	Pulse Connect Secure 9.0R3/9.1R1 and higher is vulnerable to an authentication bypass vulnerability exposed by the Windows File Share Browser and Pulse Secure Collaboration features of Pulse Connect Secure that can allow an unauthenticated user to perform remote arbitrary code execution on the Pulse Connect Secure gateway. This vulnerability has been exploited in the wild.	2021-04-23	7.5	CVE-2021-22893 MISC MISC MISC MISC
purl_project -- purl	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in purl 2.3.2 allows a malicious user to inject properties into Object.prototype.	2021-04-23	7.5	CVE-2021-20089 MISC

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acemetrix -- jquery-deparam	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-deparam 0.5.1 allows a malicious user to inject properties into Object.prototype.	2021-04-23	6.5	CVE-2021-20087 MISC
aterm -- wg2600hs_firmware	Cross-site scripting vulnerability in Aterm WG2600HS firmware Ver1.5.1 and earlier allows remote attackers to inject an arbitrary script via unspecified vectors.	2021-04-26	4.3	CVE-2021-20710 MISC MISC
avaya -- aura_orchestration_designer	An XML External Entities (XXE)vulnerability in the web-based user interface of Avaya Aura Orchestration Designer could allow an authenticated, remote attacker to gain read access to information that is stored on an affected system. The affected versions of Orchestration Designer includes all 7.x versions before 7.2.3.	2021-04-23	4	CVE-2020-7035 CONFIRM
avaya -- callback_assist	An XML External Entities (XXE)vulnerability in Callback Assist could allow an authenticated, remote attacker to gain read access to information that is stored on an affected system. The affected versions of Callback Assist includes all 4.0.x versions before 4.7.1.1 Patch 7.	2021-04-23	4	CVE-2020-7036 CONFIRM
backbone-query-parameters_project -- backbone-query-parameters	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in backbone-query-parameters 0.4.0 allows a malicious user to inject properties into Object.prototype.	2021-04-23	6.5	CVE-2021-20085 MISC
criticalmanufacturing -- cncsoft-b	CNCSoft-B Versions 1.0.0.3 and prior is vulnerable to an out-of-bounds write, which may allow an attacker to execute arbitrary code.	2021-04-27	6.8	CVE-2021-22664 MISC MISC
directum -- directum	Settings.aspx?view=About in Directum 5.8.2 allows XSS via the HTTP User-Agent header.	2021-04-24	4.3	CVE-2021-31794 MISC MISC
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions starting from 11.9. GitLab was not properly validating image files that were passed to a file parser which resulted in a remote command execution.	2021-04-23	6.5	CVE-2021-22205 MISC MISC CONFIRM
google -- chrome	Insufficient data validation in V8 in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-30	6.8	CVE-2021-21227 MISC MISC GENTOO
google -- chrome	Type confusion in V8 in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-30	6.8	CVE-2021-21230 MISC MISC GENTOO
google -- chrome	Use after free in Dev Tools in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-30	6.8	CVE-2021-21232 MISC MISC GENTOO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Type confusion in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21224 MISC MISC DEBIAN GENTOO
google -- chrome	Integer overflow in Mojo in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21223 MISC MISC DEBIAN GENTOO
google -- chrome	Use after free in Blink in Google Chrome prior to 89.0.4389.128 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21206 MISC MISC GENTOO
google -- chrome	Insufficient validation of untrusted input in V8 in Google Chrome prior to 89.0.4389.128 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21220 MISC MISC GENTOO
google -- chrome	Use after free in WebMIDI in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21213 MISC MISC DEBIAN GENTOO
google -- chrome	Use after free in IndexedDB in Google Chrome prior to 90.0.4430.72 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	2021-04-26	6.8	CVE-2021-21207 MISC MISC DEBIAN GENTOO
google -- chrome	Heap buffer overflow in ANGLE in Google Chrome on Windows prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-30	6.8	CVE-2021-21233 MISC MISC GENTOO
google -- chrome	Use after free in Blink in Google Chrome on OS X prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21204 MISC MISC DEBIAN GENTOO
google -- chrome	Use after free in Blink in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21203 MISC MISC DEBIAN GENTOO
google -- chrome	Use after free in navigation in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21226 MISC MISC DEBIAN GENTOO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Use after free in Network API in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension.	2021-04-26	6.8	CVE-2021-21214 MISC MISC DEBIAN GENTOO
google -- chrome	Out of bounds memory access in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21225 MISC MISC DEBIAN GENTOO
google -- chrome	Use after free in permissions in Google Chrome prior to 90.0.4430.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2021-04-26	6.8	CVE-2021-21201 MISC MISC DEBIAN GENTOO
google -- chrome	Incorrect security UI in Network Config UI in Google Chrome on ChromeOS prior to 90.0.4430.72 allowed a remote attacker to potentially compromise WiFi connection security via a malicious WAP.	2021-04-26	4.3	CVE-2021-21212 MISC MISC DEBIAN GENTOO
google -- chrome	Heap buffer overflow in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.	2021-04-26	4.3	CVE-2021-21222 MISC MISC DEBIAN GENTOO
google -- chrome	Inappropriate implementation in storage in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-04-26	4.3	CVE-2021-21209 MISC MISC DEBIAN GENTOO
google -- chrome	Insufficient policy enforcement in navigation in Google Chrome on iOS prior to 90.0.4430.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2021-04-26	5.8	CVE-2021-21205 MISC MISC DEBIAN GENTOO
google -- chrome	Use after free in extensions in Google Chrome prior to 90.0.4430.72 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	2021-04-26	6.8	CVE-2021-21202 MISC MISC DEBIAN GENTOO
google -- chrome	Insufficient data validation in QR scanner in Google Chrome on iOS prior to 90.0.4430.72 allowed an attacker displaying a QR code to perform domain spoofing via a crafted QR code.	2021-04-26	4.3	CVE-2021-21208 MISC MISC DEBIAN GENTOO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Inappropriate implementation in Network in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially access local UDP ports via a crafted HTML page.	2021-04-26	4.3	CVE-2021-21210 MISC MISC DEBIAN GENTOO
google -- chrome	Insufficient validation of untrusted input in Mojo in Google Chrome prior to 90.0.4430.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page.	2021-04-26	4.3	CVE-2021-21221 MISC MISC DEBIAN GENTOO
google -- chrome	Inappropriate implementation in Navigation in Google Chrome on iOS prior to 90.0.4430.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2021-04-26	4.3	CVE-2021-21211 MISC MISC DEBIAN GENTOO
google -- chrome	Inappropriate implementation in Autofill in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to spoof security UI via a crafted HTML page.	2021-04-26	4.3	CVE-2021-21215 MISC MISC DEBIAN GENTOO
google -- chrome	Inappropriate implementation in Autofill in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to spoof security UI via a crafted HTML page.	2021-04-26	4.3	CVE-2021-21216 MISC MISC DEBIAN GENTOO
google -- chrome	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.	2021-04-26	4.3	CVE-2021-21217 MISC MISC DEBIAN GENTOO
google -- chrome	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.	2021-04-26	4.3	CVE-2021-21218 MISC MISC DEBIAN GENTOO
google -- chrome	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.	2021-04-26	4.3	CVE-2021-21219 MISC MISC DEBIAN GENTOO
hornerautomation -- cscape	Cscape (All versions prior to 9.90 SP4) lacks proper validation of user-supplied data when parsing project files. This could lead to memory corruption. An attacker could leverage this vulnerability to execute code in the context of the current process.	2021-04-23	6.8	CVE-2021-22678 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hornerautomation -- cscape	Cscape (All versions prior to 9.90 SP4) is configured by default to be installed for all users, which allows full permissions, including read/write access. This may allow unprivileged users to modify the binaries and configuration files and lead to local privilege escalation.	2021-04-23	4.6	CVE-2021-22682 MISC
ibm -- informix_dynamic_server	IBM Informix Dynamic Server 14.10 is vulnerable to a stack based buffer overflow, caused by improper bounds checking. A local privileged user could overflow a buffer and execute arbitrary code on the system or cause a denial of service condition. IBM X-Force ID: 198366.	2021-04-30	4.6	CVE-2021-20515 XF CONFIRM
ibm -- planning_analytics	IBM Planning Analytics 2.0 could allow a remote attacker to obtain sensitive information by allowing cross-window communication with unrestricted target origin via documentation frames.	2021-04-26	5	CVE-2020-4562 XF CONFIRM
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 200258.	2021-04-26	5	CVE-2021-29694 XF CONFIRM
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.7 uses Cross-Origin Resource Sharing (CORS) which could allow an attacker to carry out privileged actions and retrieve sensitive information as the domain name is not being limited to only trusted domains. IBM X-Force ID: 196344.	2021-04-26	6.4	CVE-2021-20432 XF CONFIRM
jamovi -- jamovi	Jamovi <=1.6.18 is affected by a cross-site scripting (XSS) vulnerability. The column-name is vulnerable to XSS in the ElectronJS Framework. An attacker can make a .omv (Jamovi) document containing a payload. When opened by victim, the payload is triggered.	2021-04-26	4.3	CVE-2021-28079 MISC MISC
jquery-plugin-query-object_project -- jquery-plugin-query-object	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-plugin-query-object 2.2.3 allows a malicious user to inject properties into Object.prototype.	2021-04-23	6.5	CVE-2021-20083 MISC
jquery-sparkle_project -- jquery-sparkle	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in jquery-sparkle 1.5.2-beta allows a malicious user to inject properties into Object.prototype.	2021-04-23	6.5	CVE-2021-20084 MISC
minthcm -- minthcm	The Import function in MintHCM RELEASE 3.0.8 allows an attacker to execute a cross-site scripting (XSS) payload in file-upload.	2021-04-26	4.3	CVE-2021-25838 MISC MISC
mootools -- mootools-more	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') in mootools-more 1.6.0 allows a malicious user to inject properties into Object.prototype.	2021-04-23	6.5	CVE-2021-20088 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an assertion failure and denial of service in synth_cname.	2021-04-27	5	CVE-2019-25036 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an assertion failure and denial of service in dname_pkt_copy via an invalid packet.	2021-04-27	5	CVE-2019-25037 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nlnetlabs -- unbound	Unbound before 1.9.5 allows an infinite loop via a compressed name in dname_pkt_copy.	2021-04-27	5	CVE-2019-25040 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows an assertion failure via a compressed name in dname_pkt_copy.	2021-04-27	5	CVE-2019-25041 MISC
nlnetlabs -- unbound	Unbound before 1.9.5 allows configuration injection in create_unbound_ad_servers.sh upon a successful man-in-the-middle attack against a cleartext HTTP session.	2021-04-27	4.3	CVE-2019-25031 MISC
pfsense -- pfsense	pfSense 2.5.0 allows XSS via the services_wol_edit.php Description field.	2021-04-28	4.3	CVE-2021-27933 FULLDISC
webmin -- webmin	Webmin 1.973 is affected by Cross Site Request Forgery (CSRF) to achieve Remote Command Execution (RCE) through Webmin's running process feature.	2021-04-25	6.8	CVE-2021-31760 MISC MISC MISC MISC
webmin -- webmin	Webmin 1.973 is affected by reflected Cross Site Scripting (XSS) to achieve Remote Command Execution through Webmin's running process feature.	2021-04-25	6.8	CVE-2021-31761 MISC MISC MISC MISC
webmin -- webmin	Webmin 1.973 is affected by Cross Site Request Forgery (CSRF) to create a privileged user through Webmin's add users feature, and then get a reverse shell through Webmin's running process feature.	2021-04-25	6.8	CVE-2021-31762 MISC MISC MISC MISC
wireshark -- wireshark	Excessive memory consumption in MS-WSP dissector in Wireshark 3.4.0 to 3.4.4 and 3.2.0 to 3.2.12 allows denial of service via packet injection or crafted capture file	2021-04-23	5	CVE-2021-22207 CONFIRM MISC MISC
xmlhttprequest-ssl_project -- xmlhttprequest-ssl	The xmlhttprequest-ssl package before 1.6.1 for Node.js disables SSL certificate validation by default, because rejectUnauthorized (when the property exists but is undefined) is considered to be false within the https.request function of Node.js. In other words, no certificate is ever rejected.	2021-04-23	5.8	CVE-2021-31597 MISC MISC MISC

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dotcms -- dotcms	Cross Site Scripting (XSS) in dotCMS v5.1.5 allows remote attackers to execute arbitrary code by injecting a malicious payload into the "Task Detail" comment window of the "/dotAdmin/#/c/workflow" component.	2021-04-23	3.5	CVE-2020-17542 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- spectrum_protect_client	IBM Spectrum Protect Client 8.1.0.0 through 8.1.11.0 is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A local attacker could overflow a buffer and cause the application to crash. IBM X-Force ID: 198934	2021-04-26	2.1	CVE-2021-20546 XF CONFIRM
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus File Systems Agent 10.1.6 and 10.1.7 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 198836.	2021-04-26	2.1	CVE-2021-20536 CONFIRM XF
vaadin -- flow	Non-constant-time comparison of CSRF tokens in UIDL request handler in com.vaadin:flow-server versions 1.0.0 through 1.0.13 (Vaadin 10.0.0 through 10.0.16), 1.1.0 prior to 2.0.0 (Vaadin 11 prior to 14), 2.0.0 through 2.4.6 (Vaadin 14.0.0 through 14.4.6), 3.0.0 prior to 5.0.0 (Vaadin 15 prior to 18), and 5.0.0 through 5.0.2 (Vaadin 18.0.0 through 18.0.5) allows attacker to guess a security token via timing attack.	2021-04-23	1.9	CVE-2021-31404 CONFIRM CONFIRM
vaadin -- flow	Non-constant-time comparison of CSRF tokens in endpoint request handler in com.vaadin:flow-server versions 3.0.0 through 5.0.3 (Vaadin 15.0.0 through 18.0.6), and com.vaadin:fusion-endpoint version 6.0.0 (Vaadin 19.0.0) allows attacker to guess a security token for Fusion endpoints via timing attack.	2021-04-23	1.9	CVE-2021-31406 CONFIRM CONFIRM
vaadin -- vaadin	Non-constant-time comparison of CSRF tokens in UIDL request handler in com.vaadin:vaadin-server versions 7.0.0 through 7.7.23 (Vaadin 7.0.0 through 7.7.23), and 8.0.0 through 8.12.2 (Vaadin 8.0.0 through 8.12.2) allows attacker to guess a security token via timing attack	2021-04-23	1.9	CVE-2021-31403 CONFIRM CONFIRM CONFIRM
wowza -- streaming_engine	Wowza Streaming Engine through 4.8.5 (in a default installation) has incorrect file permissions of configuration files in the conf/ directory. A regular local user is able to read and write to all the configuration files, e.g., modify the application server configuration.	2021-04-23	3.6	CVE-2021-31540 MISC MISC
wowza -- streaming_engine	Wowza Streaming Engine through 4.8.5 (in a default installation) has cleartext passwords stored in the conf/admin.password file. A regular local user is able to read usernames and passwords.	2021-04-23	2.1	CVE-2021-31539 MISC MISC

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
akuvox -- c315	Akuvox C315 115.116.2613 allows remote command Injection via the cfgd_server service. The attack vector is sending a payload to port 189 (default root 0.0.0.0).	2021-04-25	not yet calculated	CVE-2021-31726 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ambarella -- oryx-rtsp_server	A buffer overflow in the RTSP service of the Ambarella Oryx RTSP Server 2020-01-07 allows an unauthenticated attacker to send a crafted RTSP request, with a long digest authentication header, to execute arbitrary code in parse_authentication_header() in libamprotocol-rtsp.so.1 in rtsp_svc (or cause a crash). This allows remote takeover of a Furbo Dog Camera, for example.	2021-04-30	not yet calculated	CVE-2020-24918 MISC MISC MISC
ampache -- ampache	Ampache before version 4.2.2 allows unauthenticated users to perform SQL injection. Refer to the referenced GitHub Security Advisory for details and a workaround. This is fixed in version 4.2.2 and the development branch.	2021-04-30	not yet calculated	CVE-2020-15153 MISC MISC CONFIRM
ansible -- engine	A flaw was found in the Ansible Engine 2.9.18, where sensitive info is not masked by default and is not protected by the no_log feature when using the sub-option feature of the basic.py module. This flaw allows an attacker to obtain sensitive information. The highest threat from this vulnerability is to confidentiality.	2021-04-29	not yet calculated	CVE-2021-20228 MISC MISC
apache -- maven	Apache Maven will follow repositories that are defined in a dependency's Project Object Model (pom) which may be surprising to some users, resulting in potential risk if a malicious actor takes over that repository or is able to insert themselves into a position to pretend to be that repository. Maven is changing the default behavior in 3.8.1+ to no longer follow http (non-SSL) repository references by default. More details available in the referenced urls. If you are currently using a repository manager to govern the repositories used by your builds, you are unaffected by the risks present in the legacy behavior, and are unaffected by this vulnerability and change to default behavior. See this link for more information about repository management: https://maven.apache.org/repository-management.html	2021-04-23	not yet calculated	CVE-2021-26291 MISC MLIST MLIST MLIST MLIST MLIST MLIST
apache -- ofbiz	Apache OFBiz has unsafe deserialization prior to 17.12.07 version	2021-04-27	not yet calculated	CVE-2021-30128 MISC MLIST MLIST MLIST MLIST MLIST MLIST MLIST
apache -- ofbiz	Apache OFBiz has unsafe deserialization prior to 17.12.07 version An unauthenticated user can perform an RCE attack	2021-04-27	not yet calculated	CVE-2021-29200 MISC MLIST MLIST MLIST MLIST MLIST MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- ozone_cluster	The S3 buckets and keys in a secure Apache Ozone Cluster must be inaccessible to anonymous access by default. The current security vulnerability allows access to keys and buckets through a curl command or an unauthenticated HTTP request. This enables unauthorized access to buckets and keys thereby exposing data to anonymous clients or users. This affected Apache Ozone prior to the 1.1.0 release. Improper Authorization vulnerability in __COMPONENT__ of Apache Ozone allows an attacker to __IMPACT__. This issue affects Apache Ozone Apache Ozone version 1.0.0 and prior versions.	2021-04-27	not yet calculated	CVE-2020-17517 MISC
apache -- superset	Apache Superset up to and including 1.0.1 allowed for the creation of an external URL that could be malicious. By not checking user input for open redirects the URL shortener functionality would allow for a malicious user to create a short URL for a dashboard that could convince the user to click the link.	2021-04-27	not yet calculated	CVE-2021-28125 MISC MLIST MLIST
apache -- tapestry	Information Exposure vulnerability in context asset handling of Apache Tapestry allows an attacker to download files inside WEB-INF if using a specially-constructed URL. This was caused by an incomplete fix for CVE-2020-13953. This issue affects Apache Tapestry Apache Tapestry 5.4.0 version to Apache Tapestry 5.6.3; Apache Tapestry 5.7.0 version and Apache Tapestry 5.7.1.	2021-04-27	not yet calculated	CVE-2021-30638 MISC MLIST MISC
aruba -- airwave_management_platform	A remote insecure deserialization vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	2021-04-28	not yet calculated	CVE-2021-25152 MISC
aruba -- airwave_management_platform	A remote SQL injection vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	2021-04-28	not yet calculated	CVE-2021-25153 MISC
aruba -- airwave_management_platform	A remote escalation of privilege vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	2021-04-28	not yet calculated	CVE-2021-25154 MISC
aruba -- airwave_management_platform	A remote XML external entity vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	2021-04-28	not yet calculated	CVE-2021-25164 MISC
aruba -- airwave_management_platform	A remote insecure deserialization vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	2021-04-28	not yet calculated	CVE-2021-25151 MISC
aruba -- airwave_management_platform	A remote URL redirection vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	2021-04-29	not yet calculated	CVE-2021-29137 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aruba -- airwave_management_platform	A remote XML external entity vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	2021-04-29	not yet calculated	CVE-2021-25163 MISC
aruba -- airwave_management_platform	A remote authentication restriction bypass vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	2021-04-28	not yet calculated	CVE-2021-25147 MISC
aruba -- airwave_management_platform	A remote unauthorized access vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	2021-04-29	not yet calculated	CVE-2021-25167 MISC
aruba -- airwave_management_platform	A remote unauthorized access vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	2021-04-29	not yet calculated	CVE-2021-25166 MISC
aruba -- airwave_management_platform	A remote XML external entity vulnerability was discovered in Aruba AirWave Management Platform version(s) prior to 8.2.12.1. Aruba has released patches for AirWave Management Platform that address this security vulnerability.	2021-04-28	not yet calculated	CVE-2021-25165 MISC
aruba -- clearpass_policy_manager	A remote disclosure of sensitive information vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	2021-04-29	not yet calculated	CVE-2021-29141 MISC
aruba -- clearpass_policy_manager	A remote disclosure of sensitive information vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	2021-04-29	not yet calculated	CVE-2021-29144 MISC
aruba -- clearpass_policy_manager	A local escalation of privilege vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	2021-04-28	not yet calculated	CVE-2020-7123 MISC
aruba -- clearpass_policy_manager	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	2021-04-29	not yet calculated	CVE-2021-29147 MISC
aruba -- clearpass_policy_manager	A remote cross-site scripting (XSS) vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	2021-04-29	not yet calculated	CVE-2021-29146 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aruba -- clearpass_policy_manager	A remote server side request forgery (SSRF) remote code execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	2021-04-29	not yet calculated	CVE-2021-29145 MISC
aruba -- clearpass_policy_manager	A remote cross-site scripting (XSS) vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	2021-04-29	not yet calculated	CVE-2021-29142 MISC
aruba -- clearpass_policy_manager	A remote XML external entity (XXE) vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	2021-04-29	not yet calculated	CVE-2021-29140 MISC
aruba -- clearpass_policy_manager	A remote cross-site scripting (XSS) vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	2021-04-29	not yet calculated	CVE-2021-29139 MISC
aruba -- clearpass_policy_manager	A remote disclosure of privileged information vulnerability was discovered in Aruba ClearPass Policy Manager version(s) prior to 6.9.5, 6.8.9, 6.7.14-HF1. Aruba has released patches for Aruba ClearPass Policy Manager that address this security vulnerability.	2021-04-29	not yet calculated	CVE-2021-29138 MISC
avava -- equinox_conferencing	A vulnerability was discovered in Management component of Avaya Equinox Conferencing that could potentially allow an unauthenticated, remote attacker to gain access to screen sharing and whiteboard sessions. The affected versions of Management component of Avaya Equinox Conferencing include all 3.x versions before 3.17. Avaya Equinox Conferencing is now offered as Avaya Meetings Server.	2021-04-28	not yet calculated	CVE-2020-7038 CONFIRM
avava -- equinox_conferencing	An XML External Entities (XXE) vulnerability in Media Server component of Avaya Equinox Conferencing could allow an authenticated, remote attacker to gain read access to information that is stored on an affected system or even potentially lead to a denial of service. The affected versions of Avaya Equinox Conferencing includes all 9.x versions before 9.1.11. Equinox Conferencing is now offered as Avaya Meetings Server.	2021-04-28	not yet calculated	CVE-2020-7037 CONFIRM
ave -- dominaplus	AVE DOMINAplus <=1.10.x suffers from clear-text credentials disclosure vulnerability that allows an unauthenticated attacker to issue a request to an unprotected directory that hosts an XML file '/xml/authClients.xml' and obtain administrative login information that allows for a successful authentication bypass attack.	2021-04-28	not yet calculated	CVE-2020-21994 EXPLOIT-DB MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ave -- dominaplus	AVE DOMINAplus <=1.10.x suffers from an unauthenticated reboot command execution. Attackers can exploit this issue to cause a denial of service scenario.	2021-04-28	not yet calculated	CVE-2020-21996 MISC EXPLOIT-DB
ave -- dominaplus	AVE DOMINAplus <=1.10.x suffers from an authentication bypass vulnerability due to missing control check when directly calling the autologin GET parameter in changeparams.php script. Setting the autologin value to 1 allows an unauthenticated attacker to permanently disable the authentication security control and access the management interface with admin privileges without providing credentials.	2021-04-28	not yet calculated	CVE-2020-21991 MISC EXPLOIT-DB
aviatrix -- vpn_client	Aviatrix VPN Client before 2.14.14 on Windows has an unquoted search path that enables local privilege escalation to the SYSTEM user, if the machine is misconfigured to allow unprivileged users to write to directories that are supposed to be restricted to administrators.	2021-04-29	not yet calculated	CVE-2021-31776 MISC MISC CONFIRM
babel -- babel	Relative Path Traversal in Babel 2.9.0 allows an attacker to load arbitrary locale files on disk and execute arbitrary code.	2021-04-29	not yet calculated	CVE-2021-20095 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bind -- bind 	In BIND 9.5.0 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.11.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.1 of the BIND 9.17 development branch, BIND servers are vulnerable if they are running an affected version and are configured to use GSS-TSIG features. In a configuration which uses BIND's default settings the vulnerable code path is not exposed, but a server can be rendered vulnerable by explicitly setting values for the tkey-gssapi-keytab or tkey-gssapi-credential configuration options. Although the default configuration is not vulnerable, GSS-TSIG is frequently used in networks where BIND is integrated with Samba, as well as in mixed-server environments that combine BIND servers with Active Directory domain controllers. For servers that meet these conditions, the ISC SPNEGO implementation is vulnerable to various attacks, depending on the CPU architecture for which BIND was built: For named binaries compiled for 64-bit platforms, this flaw can be used to trigger a buffer over-read, leading to a server crash. For named binaries compiled for 32-bit platforms, this flaw can be used to trigger a server crash due to a buffer overflow and possibly also to achieve remote code execution. We have determined that standard SPNEGO implementations are available in the MIT and Heimdal Kerberos libraries, which support a broad range of operating systems, rendering the ISC implementation unnecessary and obsolete. Therefore, to reduce the attack surface for BIND users, we will be removing the ISC SPNEGO implementation in the April releases of BIND 9.11 and 9.16 (it had already been dropped from BIND 9.17). We would not normally remove something from a stable ESV (Extended Support Version) of BIND, but since system libraries can replace the ISC SPNEGO implementation, we have made an exception in this case for reasons of stability and security.	2021-04-29	not yet calculated	CVE-2021-25216 CONFIRM MLIST MLIST MLIST MLIST DEBIAN
bind -- bind 	In BIND 9.8.5 -> 9.8.8, 9.9.3 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.9.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND 9 Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.11 of the BIND 9.17 development branch, when a vulnerable version of named receives a malformed IXFR triggering the flaw described above, the named process will terminate due to a failed assertion the next time the transferred secondary zone is refreshed.	2021-04-29	not yet calculated	CVE-2021-25214 CONFIRM MLIST MLIST MLIST MLIST DEBIAN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bind -- bind	In BIND 9.0.0 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.9.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.11 of the BIND 9.17 development branch, when a vulnerable version of named receives a query for a record triggering the flaw described above, the named process will terminate due to a failed assertion check. The vulnerability affects all currently maintained BIND 9 branches (9.11, 9.11-S, 9.16, 9.16-S, 9.17) as well as all other versions of BIND 9.	2021-04-29	not yet calculated	CVE-2021-25215 CONFIRM MLIST MLIST MLIST MLIST DEBIAN
binutils -- readelf	A flaw was found in binutils readelf 2.35 program. An attacker who is able to convince a victim using readelf to read a crafted file could trigger a stack buffer overflow, out-of-bounds write of arbitrary data supplied by the attacker. The highest impact of this flaw is to confidentiality, integrity, and availability.	2021-04-29	not yet calculated	CVE-2021-20294 MISC MISC
browserlist -- browserlist	The package browserslist from 4.0.0 and before 4.16.5 are vulnerable to Regular Expression Denial of Service (ReDoS) during parsing of queries.	2021-04-28	not yet calculated	CVE-2021-23364 MISC MISC MISC MISC MISC
buffalo -- buffalo	The web interfaces of Buffalo WSR-2533DHPL2 firmware version <= 1.02 and WSR-2533DHP3 firmware version <= 1.24 do not properly restrict access to sensitive information from an unauthorized actor.	2021-04-29	not yet calculated	CVE-2021-20092 MISC
buffalo -- buffalo	The web interfaces of Buffalo WSR-2533DHPL2 firmware version <= 1.02 and WSR-2533DHP3 firmware version <= 1.24 do not properly sanitize user input. An authenticated remote attacker could leverage this vulnerability to alter device configuration, potentially gaining remote code execution.	2021-04-29	not yet calculated	CVE-2021-20091 MISC
buffalo -- buffalo	A path traversal vulnerability in the web interfaces of Buffalo WSR-2533DHPL2 firmware version <= 1.02 and WSR-2533DHP3 firmware version <= 1.24 could allow unauthenticated remote attackers to bypass authentication.	2021-04-29	not yet calculated	CVE-2021-20090 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
buffalo -- multiple_network_devices	Hidden functionality in multiple Buffalo network devices (BHR-4RV firmware Ver.2.55 and prior, FS-G54 firmware Ver.2.04 and prior, WBR2-B11 firmware Ver.2.32 and prior, WBR2-G54 firmware Ver.2.32 and prior, WBR2-G54-KD firmware Ver.2.32 and prior, WBR-B11 firmware Ver.2.23 and prior, WBR-G54 firmware Ver.2.23 and prior, WBR-G54L firmware Ver.2.20 and prior, WHR2-A54G54 firmware Ver.2.25 and prior, WHR2-G54 firmware Ver.2.23 and prior, WHR2-G54V firmware Ver.2.55 and prior, WHR3-AG54 firmware Ver.2.23 and prior, WHR-G54 firmware Ver.2.16 and prior, WHR-G54-NF firmware Ver.2.10 and prior, WLA2-G54 firmware Ver.2.24 and prior, WLA2-G54C firmware Ver.2.24 and prior, WLA-B11 firmware Ver.2.20 and prior, WLA-G54 firmware Ver.2.20 and prior, WLA-G54C firmware Ver.2.20 and prior, WLAH-A54G54 firmware Ver.2.54 and prior, WLAH-AM54G54 firmware Ver.2.54 and prior, WLAH-G54 firmware Ver.2.54 and prior, WLI2-TX1-AG54 firmware Ver.2.53 and prior, WLI2-TX1-AMG54 firmware Ver.2.53 and prior, WLI2-TX1-G54 firmware Ver.2.20 and prior, WLI3-TX1-AMG54 firmware Ver.2.53 and prior, WLI3-TX1-G54 firmware Ver.2.53 and prior, WLI-T1-B11 firmware Ver.2.20 and prior, WLI-TX1-G54 firmware Ver.2.20 and prior, WVR-G54-NF firmware Ver.2.02 and prior, WZR-G108 firmware Ver.2.41 and prior, WZR-G54 firmware Ver.2.41 and prior, WZR-HP-G54 firmware Ver.2.41 and prior, WZR-RS-G54 firmware Ver.2.55 and prior, and WZR-RS-G54HP firmware Ver.2.55 and prior) allows a remote attacker to enable the debug option and to execute arbitrary code or OS commands, change the configuration, and cause a denial of service (DoS) condition.	2021-04-28	not yet calculated	CVE-2021-20716 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
buffalo -- multiple_routers 	Improper access control vulnerability in Buffalo broadband routers (BHR-4GRV firmware Ver.1.99 and prior, DWR-HP-G300NH firmware Ver.1.83 and prior, HW-450HP-ZWE firmware Ver.1.99 and prior, WHR-300HP firmware Ver.1.99 and prior, WHR-300 firmware Ver.1.99 and prior, WHR-G301N firmware Ver.1.86 and prior, WHR-HP-G300N firmware Ver.1.99 and prior, WHR-HP-GN firmware Ver.1.86 and prior, WPL-05G300 firmware Ver.1.87 and prior, WZR-450HP-CWT firmware Ver.1.99 and prior, WZR-450HP-UB firmware Ver.1.99 and prior, WZR-HP-AG300H firmware Ver.1.75 and prior, WZR-HP-G300NH firmware Ver.1.83 and prior, WZR-HP-G301NH firmware Ver.1.83 and prior, WZR-HP-G302H firmware Ver.1.85 and prior, WZR-HP-G450H firmware Ver.1.89 and prior, WZR-300HP firmware Ver.1.99 and prior, WZR-450HP firmware Ver.1.99 and prior, WZR-600DHP firmware Ver.1.99 and prior, WZR-D1100H firmware Ver.1.99 and prior, FS-HP-G300N firmware Ver.3.32 and prior, FS-600DHP firmware Ver.3.38 and prior, FS-R600DHP firmware Ver.3.39 and prior, and FS-G300N firmware Ver.3.13 and prior) allows remote unauthenticated attackers to bypass access restriction and to start telnet service and execute arbitrary OS commands with root privileges via unspecified vectors.	2021-04-28	not yet calculated	CVE-2021-3512 MISC MISC
buffalo -- multiple_routers 	Disclosure of sensitive information to an unauthorized user vulnerability in Buffalo broadband routers (BHR-4GRV firmware Ver.1.99 and prior, DWR-HP-G300NH firmware Ver.1.83 and prior, HW-450HP-ZWE firmware Ver.1.99 and prior, WHR-300HP firmware Ver.1.99 and prior, WHR-300 firmware Ver.1.99 and prior, WHR-G301N firmware Ver.1.86 and prior, WHR-HP-G300N firmware Ver.1.99 and prior, WHR-HP-GN firmware Ver.1.86 and prior, WPL-05G300 firmware Ver.1.87 and prior, WZR-450HP-CWT firmware Ver.1.99 and prior, WZR-450HP-UB firmware Ver.1.99 and prior, WZR-HP-AG300H firmware Ver.1.75 and prior, WZR-HP-G300NH firmware Ver.1.83 and prior, WZR-HP-G301NH firmware Ver.1.83 and prior, WZR-HP-G302H firmware Ver.1.85 and prior, WZR-HP-G450H firmware Ver.1.89 and prior, WZR-300HP firmware Ver.1.99 and prior, WZR-450HP firmware Ver.1.99 and prior, WZR-600DHP firmware Ver.1.99 and prior, WZR-D1100H firmware Ver.1.99 and prior, FS-HP-G300N firmware Ver.3.32 and prior, FS-600DHP firmware Ver.3.38 and prior, FS-R600DHP firmware Ver.3.39 and prior, and FS-G300N firmware Ver.3.13 and prior) allows remote unauthenticated attackers to obtain information such as configuration via unspecified vectors.	2021-04-28	not yet calculated	CVE-2021-3511 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bundler -- bundler	Bundler 1.16.0 through 2.2.9 and 2.2.11 through 2.2.16 sometimes chooses a dependency source based on the highest gem version number, which means that a rogue gem found at a public source may be chosen, even if the intended choice was a private gem that is a dependency of another private gem that is explicitly depended on by the application. NOTE: it is not correct to use CVE-2021-24105 for every "Dependency Confusion" issue in every product.	2021-04-29	not yet calculated	CVE-2020-36327 MISC MISC MISC MISC MISC
cesanta -- mongooseos	In mjs_json.c in Cesanta MongooseOS mJS 1.26, a maliciously formed JSON string can trigger an off-by-one heap-based buffer overflow in mjs_json_parse, which can potentially lead to redirection of control flow.	2021-04-29	not yet calculated	CVE-2021-31875 MISC MISC MISC
chamilo -- chamilo	A remote code execution vulnerability exists in Chamilo through 1.11.14 due to improper input sanitization of a parameter used for file uploads, and improper file-extension filtering for certain filenames (e.g., .phar or .pht). A remote authenticated administrator is able to upload a file containing arbitrary PHP code into specific directories via main/inc/lib/fileUpload.lib.php directory traversal to achieve PHP code execution.	2021-04-30	not yet calculated	CVE-2021-31933 MISC MISC MISC
china -- mobile_an_lianbao	Command injection vulnerability in China Mobile An Lianbao WF-1 1.01 via the 'ip' parameter with a POST request to /api/ZRQos/set_online_client.	2021-04-29	not yet calculated	CVE-2021-25812 MISC MISC MISC
china_mobile -- an_lianbao	The api/ZRAndlink/set_ZRAndlink interface in China Mobile An Lianbao WF-1 router 1.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the iandlink_proc_enable parameter.	2021-04-29	not yet calculated	CVE-2021-30228 MISC MISC MISC
china_mobile -- an_lianbao_wf-1_router	The api/zrDm/set_zrDm interface in China Mobile An Lianbao WF-1 router 1.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the dm_enable, AppKey, or Pwd parameter.	2021-04-29	not yet calculated	CVE-2021-30229 MISC MISC MISC
china_mobile -- an_lianbao_wf-1_router	The api/ZRFirmware/set_time_zone interface in China Mobile An Lianbao WF-1 router 1.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the zonename parameter.	2021-04-29	not yet calculated	CVE-2021-30230 MISC MISC MISC
china_mobile -- an_lianbao_wf-a_router	The api/ZRIGMP/set_MLD_PROXY interface in China Mobile An Lianbao WF-1 router 1.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the MLD_PROXY_WAN_CONNECT parameter.	2021-04-29	not yet calculated	CVE-2021-30234 MISC MISC MISC
china_mobile -- an_lianbao_wf-a_router	The api/zrDm/set_ZRElink interface in China Mobile An Lianbao WF-1 router 1.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the bssaddr, abiaddr, devtoken, devid, elinksync, or elink_proc_enable parameter.	2021-04-29	not yet calculated	CVE-2021-30231 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
china_mobile -- an_lianbao_wf-a_router	The api/ZRIptv/setIptvInfo interface in China Mobile An Lianbao WF-1 router 1.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the iptv_vlan parameter.	2021-04-29	not yet calculated	CVE-2021-30233 MISC MISC MISC
china_mobile -- an_lianbao_wf-a_router	The api/ZRIGMP/set_IGMP_PROXY interface in China Mobile An Lianbao WF-1 router 1.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the IGMP_PROXY_WAN_CONNECT parameter.	2021-04-29	not yet calculated	CVE-2021-30232 MISC MISC MISC
cisco -- adaptive_security_appliance_software	Multiple vulnerabilities in Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. These vulnerabilities are due to lack of proper input validation of the HTTPS request. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: This vulnerability affects only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section.	2021-04-29	not yet calculated	CVE-2021-1445 CISCO
cisco -- adaptive_security_appliance_software	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to cause a buffer overflow on an affected system. The vulnerability is due to insufficient boundary checks for specific data that is provided to the web services interface of an affected system. An attacker could exploit this vulnerability by sending a malicious HTTP request. A successful exploit could allow the attacker to cause a buffer overflow condition on the affected system, which could disclose data fragments or cause the device to reload, resulting in a denial of service (DoS) condition.	2021-04-29	not yet calculated	CVE-2021-1493 CISCO
cisco -- adaptive_security_appliance_software	A vulnerability in the upgrade process of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to inject commands that could be executed with root privileges on the underlying operating system (OS). This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by uploading a crafted upgrade package file to an affected device. A successful exploit could allow the attacker to inject commands that could be executed with root privileges on the underlying OS.	2021-04-29	not yet calculated	CVE-2021-1488 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- adaptive_security_appliance_software	A vulnerability in the SIP inspection engine of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a crash and reload of an affected device, resulting in a denial of service (DoS) condition.The vulnerability is due to a crash that occurs during a hash lookup for a SIP pinhole connection. An attacker could exploit this vulnerability by sending crafted SIP traffic through an affected device. A successful exploit could allow the attacker to cause a crash and reload of the affected device.	2021-04-29	not yet calculated	CVE-2021-1501 CISCO
cisco -- adaptive_security_appliance_software	Multiple vulnerabilities in Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. These vulnerabilities are due to lack of proper input validation of the HTTPS request. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: This vulnerability affects only specific AnyConnect and WebVPN configurations. For more information, see the Vulnerable Products section.	2021-04-29	not yet calculated	CVE-2021-1504 CISCO
cisco -- adaptive_security_appliance_software	A vulnerability in the CLI of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device. The vulnerability is due to insufficient input validation of commands that are supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input for specific commands. A successful exploit could allow the attacker to execute commands on the underlying OS with root privileges. To exploit this vulnerability, an attacker must have valid administrator-level credentials.	2021-04-29	not yet calculated	CVE-2021-1476 CISCO
cisco -- firepower_device_manager	A vulnerability in the REST API of Cisco Firepower Device Manager (FDM) On-Box Software could allow an authenticated, remote attacker to gain read and write access to information that is stored on an affected device. This vulnerability is due to the improper handling of XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by sending malicious requests that contain references in XML entities to an affected system. A successful exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of sensitive information or causing a partial denial of service (DoS) condition on the affected device.	2021-04-29	not yet calculated	CVE-2021-1369 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- firepower_device_manager_software	A vulnerability in filesystem usage management for Cisco Firepower Device Manager (FDM) Software could allow an authenticated, remote attacker to exhaust filesystem resources, resulting in a denial of service (DoS) condition on an affected device. This vulnerability is due to the insufficient management of available filesystem resources. An attacker could exploit this vulnerability by uploading files to the device and exhausting available filesystem resources. A successful exploit could allow the attacker to cause database errors and cause the device to become unresponsive to web-based management. Manual intervention is required to free filesystem resources and return the device to an operational state.	2021-04-29	not yet calculated	CVE-2021-1489 CISCO
cisco -- firepower_management_center_software	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	2021-04-29	not yet calculated	CVE-2021-1458 CISCO
cisco -- firepower_management_center_software	A vulnerability in an access control mechanism of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to access services beyond the scope of their authorization. This vulnerability is due to insufficient enforcement of access control in the affected software. An attacker could exploit this vulnerability by directly accessing the internal services of an affected device. A successful exploit could allow the attacker to overwrite policies and impact the configuration and operation of the affected device.	2021-04-29	not yet calculated	CVE-2021-1477 CISCO
cisco -- firepower_management_center_software	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	2021-04-29	not yet calculated	CVE-2021-1456 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- firepower_management_center_software	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	2021-04-29	not yet calculated	CVE-2021-1457 CISCO
cisco -- firepower_managment_center_software	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	2021-04-29	not yet calculated	CVE-2021-1455 CISCO
cisco -- firepower_threat_defense_software	A vulnerability in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to overwrite files on the file system of an affected device by using directory traversal techniques. A successful exploit could cause system instability if important system files are overwritten. This vulnerability is due to insufficient validation of user input for the file path in a specific CLI command. An attacker could exploit this vulnerability by logging in to a targeted device and issuing a specific CLI command with crafted user input. A successful exploit could allow the attacker to overwrite arbitrary files on the file system of the affected device. The attacker would need valid user credentials on the device.	2021-04-29	not yet calculated	CVE-2021-1256 CISCO
cisco -- firepower_threat_defense_software	A vulnerability in the software-based SSL/TLS message handler of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient validation of SSL/TLS messages when the device performs software-based SSL decryption. An attacker could exploit this vulnerability by sending a crafted SSL/TLS message through an affected device. SSL/TLS messages sent to an affected device do not trigger this vulnerability. A successful exploit could allow the attacker to cause a process to crash. This crash would then trigger a reload of the device. No manual intervention is needed to recover the device after the reload.	2021-04-29	not yet calculated	CVE-2021-1402 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- firepower_threat_defense_software	A vulnerability in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary commands with root privileges on the underlying operating system of an affected device that is running in multi-instance mode. This vulnerability is due to insufficient validation of user-supplied command arguments. An attacker could exploit this vulnerability by submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges.	2021-04-29	not yet calculated	CVE-2021-1448 CISCO
cisco -- multiple_products	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of specific HTTP header parameters. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured file policy for HTTP packets and deliver a malicious payload.	2021-04-29	not yet calculated	CVE-2021-1495 CISCO
ckeditor -- ckeditor	CKEditor 5 provides a WYSIWYG editing solution. This CVE affects the following npm packages: ckeditor5-engine, ckeditor5-font, ckeditor5-image, ckeditor5-list, ckeditor5-markdown-gfm, ckeditor5-media-embed, ckeditor5-paste-from-office, and ckeditor5-widget. Following an internal audit, a regular expression denial of service (ReDoS) vulnerability has been discovered in multiple CKEditor 5 packages. The vulnerability allowed to abuse particular regular expressions, which could cause a significant performance drop resulting in a browser tab freeze. It affects all users using the CKEditor 5 packages listed above at version <= 26.0.0. The problem has been recognized and patched. The fix will be available in version 27.0.0.	2021-04-29	not yet calculated	CVE-2021-21391 MISC MISC MISC MISC CONFIRM MISC MISC MISC MISC
cloudengine -- multiple_devices	There is a denial of service vulnerability in some versions of CloudEngine 5800, CloudEngine 6800, CloudEngine 7800 and CloudEngine 12800. The affected product cannot deal with some messages because of module design weakness . Attackers can exploit this vulnerability by sending a large amount of specific messages to cause denial of service. This can compromise normal service.	2021-04-28	not yet calculated	CVE-2021-22393 MISC
cloudengine -- multiple_devices	There is a pointer double free vulnerability in some versions of CloudEngine 5800, CloudEngine 6800, CloudEngine 7800 and CloudEngine 12800. When a function is called, the same memory pointer is copied to two functional modules. Attackers can exploit this vulnerability by performing a malicious operation to cause the pointer double free. This may lead to module crash, compromising normal service.	2021-04-28	not yet calculated	CVE-2021-22332 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cncf -- cortex	The Alertmanager in CNCF Cortex before 1.8.1 has a local file disclosure vulnerability when -experimental.alertmanager.enable-api is used. The HTTP basic auth password_file can be used as an attack vector to send any file content via a webhook. The alertmanager templates can be used as an attack vector to send any file content because the alertmanager can load any text file specified in the templates list.	2021-04-30	not yet calculated	CVE-2021-31232 MISC MISC MISC MISC
cncsoft-b -- cncsoft-b	CNCSoft-B Versions 1.0.0.3 and prior is vulnerable to an out-of-bounds read, which may allow an attacker to execute arbitrary code.	2021-04-27	not yet calculated	CVE-2021-22660 MISC MISC MISC
composer -- composer	Composer is a dependency manager for PHP. URLs for Mercurial repositories in the root composer.json and package source download URLs are not sanitized correctly. Specifically crafted URL values allow code to be executed in the HgDriver if hg/Mercurial is installed on the system. The impact to Composer users directly is limited as the composer.json file is typically under their own control and source download URLs can only be supplied by third party Composer repositories they explicitly trust to download and execute source code from, e.g. Composer plugins. The main impact is to services passing user input to Composer, including Packagist.org and Private Packagist. This allowed users to trigger remote code execution. The vulnerability has been patched on Packagist.org and Private Packagist within 12h of receiving the initial vulnerability report and based on a review of logs, to the best of our knowledge, was not abused by anyone. Other services/tools using VcsRepository/VcsDriver or derivatives may also be vulnerable and should upgrade their composer/composer dependency immediately. Versions 1.10.22 and 2.0.13 include patches for this issue.	2021-04-27	not yet calculated	CVE-2021-29472 MISC CONFIRM DEBIAN
cpanel -- cpanel	cPanel before 94.0.3 allows self-XSS via EasyApache 4 Save Profile (SEC-581).	2021-04-26	not yet calculated	CVE-2021-31803 MISC
cubecoders -- application_deployment_service	AMP Application Deployment Service in CubeCoders AMP 2.1.x before 2.1.1.2 allows a remote, authenticated user to open ports in the local system firewall by crafting an HTTP(S) request directly to the applicable API endpoint (despite not having permission to make changes to the system's network configuration).	2021-04-30	not yet calculated	CVE-2021-31926 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cumulative-distribution-function -- cumulative-distribution-function	cumulative-distribution-function is an open source npm library used which calculates statistical cumulative distribution function from data array of x values. In versions prior to 2.0.0 apps using this library on improper data may crash or go into an infinite-loop. In the case of a nodejs server-app using this library to act on invalid non-numeric data, the nodejs server may crash. This may affect other users of this server and/or require the server to be rebooted for proper operation. In the case of a browser app using this library to act on invalid non-numeric data, that browser may crash or lock up. A flaw enabling an infinite-loop was discovered in the code for evaluating the cumulative-distribution-function of input data. Although the documentation explains that numeric data is required, some users may confuse an array of strings like ["1","2","3","4","5"] for numeric data [1,2,3,4,5] when it is in fact string data. An infinite loop is possible when the cumulative-distribution-function is evaluated for a given point when the input data is string data rather than type `number`. This vulnerability enables an infinite-cpu-loop denial-of-service-attack on any app using npm:cumulative-distribution-function v1.0.3 or earlier if the attacker can supply malformed data to the library. The vulnerability could also manifest if a data source to be analyzed changes data type from Arrays of number (proper) to Arrays of string (invalid, but undetected by earlier version of the library). Users should upgrade to at least v2.0.0, or the latest version. Tests for several types of invalid data have been created, and version 2.0.0 has been tested to reject this invalid data by throwing a `TypeError()` instead of processing it. Developers using this library may wish to adjust their app's code slightly to better tolerate or handle this TypeError. Apps performing proper numeric data validation before sending data to this library should be mostly unaffected by this patch. The vulnerability can be mitigated in older versions by ensuring that only finite numeric data of type `Array[number]` or `number` is passed to `cumulative-distribution-function` and its `f(x)` function, respectively.	2021-04-30	not yet calculated	CVE-2021-29486 MISC MISC CONFIRM MISC
cygwin -- cygwin	Cygwin Git is a patch set for the git command line tool for the cygwin environment. A specially crafted repository that contains symbolic links as well as files with backslash characters in the file name may cause just-checked out code to be executed while checking out a repository using Git on Cygwin. The problem will be patched in the Cygwin Git v2.31.1-2 release. At time of writing, the vulnerability is present in the upstream Git source code; any Cygwin user who compiles Git for themselves from upstream sources should manually apply a patch to mitigate the vulnerability. As mitigation users should not clone or pull from repositories from untrusted sources. CVE-2019-1354 was an equivalent vulnerability in Git for Visual Studio.	2021-04-29	not yet calculated	CVE-2021-29468 MISC MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
d-link -- dap-1880ac_firmware	DAP-1880AC firmware version 1.21 and earlier allows a remote authenticated attacker to execute arbitrary OS commands by sending a specially crafted request to a specific CGI program.	2021-04-26	not yet calculated	CVE-2021-20696 MISC MISC
d-link -- dap-1880ac_firmware	Improper access control vulnerability in DAP-1880AC firmware version 1.21 and earlier allows a remote authenticated attacker to bypass access restriction and to start a telnet service via unspecified vectors.	2021-04-26	not yet calculated	CVE-2021-20694 MISC MISC
d-link -- dap-1880ac_firmware	Improper following of a certificate's chain of trust vulnerability in DAP-1880AC firmware version 1.21 and earlier allows a remote authenticated attacker to gain root privileges via unspecified vectors.	2021-04-26	not yet calculated	CVE-2021-20695 MISC MISC
d-link -- dap-1880ac_firmware	Missing authentication for critical function in DAP-1880AC firmware version 1.21 and earlier allows a remote attacker to login to the device as an authenticated user without the access privilege via unspecified vectors.	2021-04-26	not yet calculated	CVE-2021-20697 MISC MISC
dell -- emc_idrac9	Dell EMC iDRAC9 versions prior to 4.40.00.00 contain a Time-of-check Time-of-use (TOCTOU) race condition vulnerability. A remote authenticated attacker could potentially exploit this vulnerability to gain elevated privileges when a user with higher privileges is simultaneously accessing iDRAC through the web interface.	2021-04-30	not yet calculated	CVE-2021-21539 MISC
dell -- emc_idrac9	Dell EMC iDRAC9 versions prior to 4.40.00.00 contain multiple stored cross-site scripting vulnerabilities. A remote authenticated malicious user with high privileges could potentially exploit these vulnerabilities to store malicious HTML or JavaScript code through multiple affected parameters. When victim users access the submitted data through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application.	2021-04-30	not yet calculated	CVE-2021-21543 MISC
dell -- emc_idrac9	Dell EMC iDRAC9 versions prior to 4.40.00.00 contain an improper authentication vulnerability. A remote authenticated malicious user with high privileges could potentially exploit this vulnerability to manipulate the username field under the comment section and set the value to any user.	2021-04-30	not yet calculated	CVE-2021-21544 MISC
dell -- emc_idrac9	Dell EMC iDRAC9 versions prior to 4.40.00.00 contain a DOM-based cross-site scripting vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by tricking a victim application user to supply malicious HTML or JavaScript code to DOM environment in the browser. The malicious code is then executed by the web browser in the context of the vulnerable web application.	2021-04-30	not yet calculated	CVE-2021-21541 MISC
dell -- emc_idrac9	Dell EMC iDRAC9 versions prior to 4.40.00.00 contain a stack-based overflow vulnerability. A remote authenticated attacker could potentially exploit this vulnerability to overwrite configuration information by injecting arbitrarily large payload.	2021-04-30	not yet calculated	CVE-2021-21540 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- emc_idrac9	Dell EMC iDRAC9 versions prior to 4.40.10.00 contain multiple stored cross-site scripting vulnerabilities. A remote authenticated malicious user with high privileges could potentially exploit these vulnerabilities to store malicious HTML or JavaScript code through multiple affected while generating a certificate. When victim users access the submitted data through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable application.	2021-04-30	not yet calculated	CVE-2021-21542 MISC
dell -- emc_networking_x-series	Dell EMC Networking X-Series firmware versions prior to 3.0.1.8 and Dell EMC PowerEdge VRTX Switch Module firmware versions prior to 2.0.0.82 contain a Weak Password Encryption Vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable system with privileges of the compromised account.	2021-04-30	not yet calculated	CVE-2021-21507 CONFIRM
dell -- emc_unity	Dell EMC Unity, UnityVSA, and Unity XT versions prior to 5.0.7.0.5.008 contain a plain-text password storage vulnerability when the Dell Upgrade Readiness Utility is run on the system. The credentials of the Unisphere Administrator are stored in plain text. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user.	2021-04-30	not yet calculated	CVE-2021-21547 CONFIRM
dell -- hybrid_client	Dell Hybrid Client versions prior to 1.5 contain a missing authentication for a critical function vulnerability. A local unauthenticated attacker may exploit this vulnerability in order to gain root level access to the system.	2021-04-30	not yet calculated	CVE-2021-21535 MISC
dell -- hybrid_client	Dell Hybrid Client versions prior to 1.5 contain an information exposure vulnerability. A local unauthenticated attacker may exploit this vulnerability in order to gain access to sensitive information via the local API.	2021-04-30	not yet calculated	CVE-2021-21534 MISC
dell -- hybrid_client	Dell Hybrid Client versions prior to 1.5 contain an information exposure vulnerability. A local unauthenticated attacker may exploit this vulnerability in order to register the client to a server in order to view sensitive information.	2021-04-30	not yet calculated	CVE-2021-21536 MISC
dell -- hybrid_client	Dell Hybrid Client versions prior to 1.5 contain an information exposure vulnerability. A local unauthenticated attacker may exploit this vulnerability in order to view and exfiltrate sensitive information on the system.	2021-04-30	not yet calculated	CVE-2021-21537 MISC
dell -- openmanage_enterprise-modular	Dell OpenManage Enterprise-Modular (OME-M) versions prior to 1.30.00 contain a security bypass vulnerability. An authenticated malicious user with low privileges may potentially exploit the vulnerability to escape from the restricted environment and gain access to sensitive information in the system, resulting in information disclosure and elevation of privilege.	2021-04-30	not yet calculated	CVE-2021-21530 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- unisphere	Dell Unisphere for PowerMax versions prior to 9.2.1.6 contain an Authorization Bypass Vulnerability. A local authenticated malicious user with monitor role may exploit this vulnerability to perform unauthorized actions.	2021-04-30	not yet calculated	CVE-2021-21531 CONFIRM
delta -- industrial_automation	Delta Industrial Automation COMMGR Versions 1.12 and prior are vulnerable to a stack-based buffer overflow, which may allow an attacker to execute remote code.	2021-04-27	not yet calculated	CVE-2021-27480 MISC
django -- django	django-filter is a generic system for filtering Django QuerySets based on user selections. In django-filter before version 2.4.0, automatically generated `NumberFilter` instances, whose value was later converted to an integer, were subject to potential DoS from maliciously input using exponential format with sufficiently large exponents. Version 2.4.0+ applies a `MaxValueValidator` with a a default `limit_value` of 1e50 to the form field used by `NumberFilter` instances. In addition, `NumberFilter` implements the new `get_max_validator()` which should return a configured validator instance to customise the limit, or else `None` to disable the additional validation. Users may manually apply an equivalent validator if they are not able to upgrade.	2021-04-29	not yet calculated	CVE-2020-15225 CONFIRM MISC MISC MISC
doc -- doc	SQL injection in the getip function in conn/function.php in ??100-???????? 1.1 allows remote attackers to inject arbitrary SQL commands via the X-Forwarded-For header to admin/product_add.php.	2021-04-29	not yet calculated	CVE-2021-29350 MISC
dreamforver -- simple_ghc	The unofficial vscode-ghc-simple (aka Simple Glasgow Haskell Compiler) extension before 0.2.3 for Visual Studio Code allows remote code execution via a crafted workspace configuration with replCommand.	2021-04-25	not yet calculated	CVE-2021-30502 MISC MISC CONFIRM CONFIRM
edimax -- wireless_network_camera	The default administrator account & password of the EDIMAX wireless network camera is hard-coded. Remote attackers can disassemble firmware to obtain the privileged permission and further control the devices.	2021-04-27	not yet calculated	CVE-2021-30165 CONFIRM
edimax -- wireless_network_camera	The manage users profile services of the network camera device allows an authenticated. Remote attackers can modify URL parameters and further amend user’s information and escalate privileges to control the devices.	2021-04-28	not yet calculated	CVE-2021-30167 MISC MISC MISC MISC
edimax -- wireless_network_camera	The sensitive information of webcam device is not properly protected. Remote attackers can unauthentically grant administrator’s credential and further control the devices.	2021-04-28	not yet calculated	CVE-2021-30168 MISC MISC MISC MISC
emlog -- emlog	Cross Site Scripting (XSS) vulnerability in the article comments feature in emlog 6.0.	2021-04-29	not yet calculated	CVE-2021-30227 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
emmanuel -- mydomoathome	Emmanuel MyDomoAtHome (MDAH) REST API REST API Domoticz ISS Gateway 0.2.40 is affected by an information disclosure vulnerability due to improper access control enforcement. An unauthenticated remote attacker can exploit this, via a specially crafted request to gain access to sensitive information.	2021-04-29	not yet calculated	CVE-2020-21990 EXPLOIT-DB MISC
etherpad -- etherpad	Etherpad < 1.8.3 is affected by a missing lock check which could cause a denial of service. Aggressively targeting random pad import endpoints with empty data would flatten all pads due to lack of rate limiting and missing ownership check.	2021-04-28	not yet calculated	CVE-2020-22785 CONFIRM
etherpad -- etherpad	In Etherpad UeberDB < 0.4.4, due to MySQL omitting trailing spaces on char / varchar columns during comparisons, retrieving database records using UeberDB's MySQL connector could allow bypassing access controls enforced on key names.	2021-04-28	not yet calculated	CVE-2020-22784 CONFIRM
etherpad -- etherpad	Etherpad <1.8.3 stored passwords used by users insecurely in the database and in log files. This affects every database backend supported by Etherpad.	2021-04-28	not yet calculated	CVE-2020-22783 CONFIRM MISC
etherpad -- etherpad	In Etherpad < 1.8.3, a specially crafted URI would raise an unhandled exception in the cache mechanism and cause a denial of service (crash the instance).	2021-04-28	not yet calculated	CVE-2020-22781 CONFIRM
etherpad -- etherpad	Etherpad < 1.8.3 is affected by a denial of service in the import functionality. Upload of binary file to the import endpoint would crash the instance.	2021-04-28	not yet calculated	CVE-2020-22782 CONFIRM
exiv2 -- exiv2	Exiv2 is a C++ library and a command-line utility to read, write, delete and modify Exif, IPTC, XMP and ICC image metadata. An out-of-bounds read was found in Exiv2 versions v0.27.3 and earlier. Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. The out-of-bounds read is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service by crashing Exiv2, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when writing the metadata, which is a less frequently used Exiv2 operation than reading the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as `insert`. The bug is fixed in version v0.27.4. Please see our security policy for information about Exiv2 security.	2021-04-26	not yet calculated	CVE-2021-29473 MISC CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
exiv2 -- exiv2	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 versions v0.27.3 and earlier. The out-of-bounds read is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service by crashing Exiv2, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when writing the metadata, which is a less frequently used Exiv2 operation than reading the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as `insert`. The bug is fixed in version v0.27.4.	2021-04-30	not yet calculated	CVE-2021-29463 MISC CONFIRM
exiv2 -- exiv2	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 versions v0.27.3 and earlier. The out-of-bounds read is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service by crashing Exiv2, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when writing the metadata, which is a less frequently used Exiv2 operation than reading the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as insert. The bug is fixed in version v0.27.4.	2021-04-23	not yet calculated	CVE-2021-29470 CONFIRM MISC
exiv2 -- exiv2	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A heap buffer overflow was found in Exiv2 versions v0.27.3 and earlier. The heap overflow is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to gain code execution, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when writing the metadata, which is a less frequently used Exiv2 operation than reading the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as `insert`. The bug is fixed in version v0.27.4.	2021-04-30	not yet calculated	CVE-2021-29464 MISC CONFIRM
filterediterator -- filterediterator	Requests is a HTTP library written in PHP. Requests mishandles deserialization in FilteredIterator. The issue has been patched and users of `Requests` 1.6.0, 1.6.1 and 1.7.0 should update to version 1.8.0.	2021-04-27	not yet calculated	CVE-2021-29476 CONFIRM MISC
fluidsynth -- fuidsynth	fluidsynth is a software synthesizer based on the SoundFont 2 specifications. A use after free violation was discovered in fluidsynth, that can be triggered when loading an invalid SoundFont file.	2021-04-29	not yet calculated	CVE-2021-21417 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fme -- server	Authenticated Stored XSS in FME Server versions 2019.2 and 2020.0 Beta allows a remote attacker to execute codeby injecting arbitrary web script or HTML via modifying the name of the users. The XSS is executed when an administrator access the logs.	2021-04-28	not yet calculated	CVE-2020-22790 MISC
fme -- server	Unauthenticated Stored XSS in FME Server versions 2019.2 and 2020.0 Beta allows a remote attacker to gain admin privileges by injecting arbitrary web script or HTML via the login page. The XSS is executed when an administrator accesses the logs.	2021-04-28	not yet calculated	CVE-2020-22789 MISC
foxit -- studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.931. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPM files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12377.	2021-04-29	not yet calculated	CVE-2021-31434 MISC MISC
foxit -- studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.931. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of PSP files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12443.	2021-04-29	not yet calculated	CVE-2021-31438 MISC MISC
foxit -- studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.931. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of SGI files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12376.	2021-04-29	not yet calculated	CVE-2021-31436 MISC MISC
foxit -- studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.931. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CMP files. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12331.	2021-04-29	not yet calculated	CVE-2021-31435 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
foxit -- studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.931. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of ARW files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12333.	2021-04-29	not yet calculated	CVE-2021-31433 MISC MISC
foxit -- studio_photo	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Studio Photo 3.6.6.931. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JP2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12384.	2021-04-29	not yet calculated	CVE-2021-31437 MISC MISC
freeipa -- freeipa	A smart proxy that provides a restful API to various sub-systems of the Foreman is affected by the flaw which can cause a Man-in-the-Middle attack. The FreeIPA module of Foreman smart proxy does not check the SSL certificate, thus, an unauthenticated attacker can perform actions in FreeIPA if certain conditions are met. The highest threat from this flaw is to system confidentiality. This flaw affects Foreman versions before 2.5.0.	2021-04-26	not yet calculated	CVE-2021-3494 MISC
galaxyclient -- galaxyclient	GalaxyClient version 2.0.28.9 loads unsigned DLLs such as zlib1.dll, libgcc_s_dw2-1.dll and libwinpthread-1.dll from PATH, which allows an attacker to potentially run code locally through unsigned DLL loading.	2021-04-30	not yet calculated	CVE-2021-26807 MISC MISC
gestsup -- gestsup	Gestsup before 3.2.10 allows account takeover through the password recovery functionality (remote). The affected component is the file forgot_pwd.php - it uses a weak algorithm for the generation of password recovery tokens (the PHP uniqueid function), allowing a brute force attack.	2021-04-26	not yet calculated	CVE-2021-31646 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ghost -- ghost	Ghost is a Node.js CMS. An unused endpoint added during the development of 4.0.0 has left sites vulnerable to untrusted users gaining access to Ghost Admin. Attackers can gain access by getting logged in users to click a link containing malicious code. Users do not need to enter credentials and may not know they've visited a malicious site. Ghost(Pro) has already been patched. We can find no evidence that the issue was exploited on Ghost(Pro) prior to the patch being added. Self-hosters are impacted if running Ghost a version between 4.0.0 and 4.3.2. Immediate action should be taken to secure your site. The issue has been fixed in 4.3.3, all 4.x sites should upgrade as soon as possible. As the endpoint is unused, the patch simply removes it. As a workaround blocking access to /ghost/preview can also mitigate the issue.	2021-04-29	not yet calculated	CVE-2021-29484 MISC MISC CONFIRM
gitee -- gitee	Directory Traversal in the fileDownload function in com/java2nb/common/controller/FileController.java in Novel-plus (?????-plus) 3.5.1 allows attackers to read arbitrary files via the filePath parameter.	2021-04-29	not yet calculated	CVE-2021-30048 MISC MISC
gnu -- wget	GNU Wget through 1.21.1 does not omit the Authorization header upon a redirect to a different origin, a related issue to CVE-2018-1000007.	2021-04-29	not yet calculated	CVE-2021-31879 MISC
google -- android	GAEN (aka Google/Apple Exposure Notifications) through 2021-04-27 on Android allows attackers to obtain sensitive information, such as a user's location history, in-person social graph, and (sometimes) COVID-19 infection status, because Rolling Proximity Identifiers and MAC addresses are written to the Android system log, and many Android devices have applications (preinstalled by the hardware manufacturer or network operator) that read system log data and send it to third parties. NOTE: a news outlet (The Markup) states that they received a vendor response indicating that fix deployment "began several weeks ago and will be complete in the coming days."	2021-04-28	not yet calculated	CVE-2021-31815 MISC MISC
google -- chrome	Incorrect security UI in downloads in Google Chrome on Android prior to 90.0.4430.93 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2021-04-30	not yet calculated	CVE-2021-21229 MISC MISC GENTOO
google -- chrome	Insufficient data validation in V8 in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-04-30	not yet calculated	CVE-2021-21231 MISC MISC GENTOO
google -- chrome	Insufficient policy enforcement in extensions in Google Chrome prior to 90.0.4430.93 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.	2021-04-30	not yet calculated	CVE-2021-21228 MISC MISC GENTOO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
grafana -- enterprise_metrics	The Alertmanager in Grafana Enterprise Metrics before 1.2.1 and Metrics Enterprise 1.2.1 has a local file disclosure vulnerability when experimental.alertmanager.enable-api is used. The HTTP basic auth password_file can be used as an attack vector to send any file content via a webhook. The alertmanager templates can be used as an attack vector to send any file content because the alertmanager can load any text file specified in the templates list.	2021-04-30	not yet calculated	CVE-2021-31231 MISC MISC MISC MISC
graphviz -- graph_visualization_tools	Buffer Overflow in Graphviz Graph Visualization Tools from commit ID f8b9e035 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (application crash) by loading a crafted file into the "lib/common/shapes.c" component.	2021-04-29	not yet calculated	CVE-2020-18032 MISC
guix-daemon -- guix-daemon	A security vulnerability that can lead to local privilege escalation has been found in 'guix-daemon'. It affects multi-user setups in which 'guix-daemon' runs locally. The attack consists in having an unprivileged user spawn a build process, for instance with `guix build`, that makes its build directory world-writable. The user then creates a hardlink to a root-owned file such as /etc/shadow in that build directory. If the user passed the --keep-failed option and the build eventually fails, the daemon changes ownership of the whole build tree, including the hardlink, to the user. At that point, the user has write access to the target file. Versions after and including v0.11.0-3298-g2608e40988, and versions prior to v1.2.0-75109-g94f0312546 are vulnerable.	2021-04-26	not yet calculated	CVE-2021-27851 MISC MISC
gurunavi -- gurunavi	Improper access control vulnerability in Gurunavi App for Android ver.10.0.10 and earlier and for iOS ver.11.1.2 and earlier allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App.	2021-04-26	not yet calculated	CVE-2021-20693 MISC
hame -- sd1_wifi_firmware	An access control vulnerability in Hame SD1 Wi-Fi firmware <=V.20140224154640 allows an attacker to get system administrator through an open Telnet service.	2021-04-26	not yet calculated	CVE-2021-26797 MISC
hardware_sentry -- km	In Hardware Sentry KM before 10.0.01 for BMC PATROL, a cleartext password may be discovered after a failure or timeout of a command.	2021-04-23	not yet calculated	CVE-2021-31791 MISC
hdrblobnit -- hdrblobnit	A flaw was found in RPM's hdrblobInit() in lib/header.c. This flaw allows an attacker who can modify the rpmdb to cause an out-of-bounds read. The highest threat from this vulnerability is to system availability.	2021-04-30	not yet calculated	CVE-2021-20266 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hedgedoc -- hedgedoc	HedgeDoc (formerly known as CodiMD) is an open-source collaborative markdown editor. An attacker is able to receive arbitrary files from the file system when exporting a note to PDF. Since the code injection has to take place as note content, there fore this exploit requires the attackers ability to modify a note. This will affect all instances, which have pdf export enabled. This issue has been fixed by https://github.com/hedgedoc/hedgedoc/commit/c1789474020a6d668d616464cb2da5e90e12 and is available in version 1.5.0. Starting the CodiMD/HedgeDoc instance with `CMD_ALLOW_PDF_EXPORT=false` or set `"allowPDFExport": false` in config.json can mitigate this issue for those who cannot upgrade. This exploit works because while PhantomJS doesn't actually render the `file:///` references to the PDF file itself, it still uses them internally, and exfiltration is possible, and easy through JavaScript rendering. The impact is pretty bad, as the attacker is able to read the CodiMD/HedgeDoc `config.json` file as well any other files on the filesystem. Even though the suggested Docker deploy option doesn't have many interesting files itself, the `config.json` still often contains sensitive information, database credentials, and maybe OAuth secrets among other things.	2021-04-26	not yet calculated	CVE-2021-29475 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hedgedoc -- hedgedoc	HedgeDoc (formerly known as CodiMD) is an open-source collaborative markdown editor. An attacker can read arbitrary `.md` files from the server's filesystem due to an improper input validation, which results in the ability to perform a relative path traversal. To verify if you are affected, you can try to open the following URL: `http://localhost:3000/..%2F..%2FREADME#` (replace `http://localhost:3000` with your instance's base-URL e.g. `https://demo.hedgedoc.org/..%2F..%2FREADME#`). If you see a README page being rendered, you run an affected version. The attack works due the fact that the internal router passes the url-encoded alias to the `noteController.showNote`-function. This function passes the input directly to findNote() utility function, that will pass it on the the parseNoteId()-function, that tries to make sense out of the noteId/alias and check if a note already exists and if so, if a corresponding file on disk was updated. If no note exists the note creation-function is called, which pass this unvalidated alias, with a `.md` appended, into a path.join()-function which is read from the filesystem in the follow up routine and provides the pre-filled content of the new note. This allows an attacker to not only read arbitrary `.md` files from the filesystem, but also observes changes to them. The usefulness of this attack can be considered limited, since mainly markdown files are use the file-ending `.md` and all markdown files contained in the hedgedoc project, like the README, are public anyway. If other protections such as a chroot or container or proper file permissions are in place, this attack's usefulness is rather limited. On a reverse-proxy level one can force a URL-decode, which will prevent this attack because the router will not accept such a path.	2021-04-26	not yet calculated	CVE-2021-29474 CONFIRM
homeautomation -- homeautomation	HomeAutomation 3.3.2 suffers from an authentication bypass vulnerability when spoofing client IP address using the X-Forwarded-For header with the local (loopback) IP address value allowing remote control of the smart home solution.	2021-04-27	not yet calculated	CVE-2020-22001 EXPLOIT-DB MISC
homeautomation -- homeautomation	HomeAutomation 3.3.2 suffers from an authenticated OS command execution vulnerability using custom command v0.1 plugin. This can be exploited with a CSRF vulnerability to execute arbitrary shell commands as the web user via the 'set_command_on' and 'set_command_off' POST parameters in '/system/systemplugins/customcommand/customcommand.plugin.php' by using an unsanitized PHP exec() function.	2021-04-27	not yet calculated	CVE-2020-22000 MISC EXPLOIT-DB
homeautomation -- homeautomation	HomeAutomation 3.3.2 is affected by persistent Cross Site Scripting (XSS). XSS vulnerabilities occur when input passed via several parameters to several scripts is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session.	2021-04-27	not yet calculated	CVE-2020-21987 EXPLOIT-DB MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
homeautomation -- homeautomation	HomeAutomation 3.3.2 is affected by Cross Site Request Forgery (CSRF). The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site.	2021-04-27	not yet calculated	CVE-2020-21989 EXPLOIT-DB MISC
homeautomation -- homeautomation	In HomeAutomation 3.3.2 input passed via the 'redirect' GET parameter in 'api.php' script is not properly verified before being used to redirect users. This can be exploited to redirect a user to an arbitrary website e.g. when a user clicks a specially crafted link to the affected script hosted on a trusted domain.	2021-04-27	not yet calculated	CVE-2020-21998 MISC MISC
hot_pepper -- gourmet_app	Improper access control vulnerability in Hot Pepper Gourmet App for Android ver.4.111.0 and earlier, and for iOS ver.4.111.0 and earlier allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App.	2021-04-27	not yet calculated	CVE-2021-20715 MISC
huawei -- multiple_smart_phones	There is an arbitrary memory write vulnerability in Huawei smart phone when processing file parsing. Due to insufficient validation of the input files, successful exploit could cause certain service abnormal. Affected product versions include:HUAWEI P30 versions 10.0.0.186(C10E7R5P1), 10.0.0.186(C461E4R3P1), 10.0.0.188(C00E85R2P11), 10.0.0.188(C01E88R2P11),10.0.0.188(C605E19R1P3), 10.0.0.190(C185E4R7P1), 10.0.0.190(C431E22R2P5), 10.0.0.190(C432E22R2P5),10.0.0.190(C605E19R1P3), 10.0.0.190(C636E4R3P4), 10.0.0.192(C635E3R2P4).	2021-04-28	not yet calculated	CVE-2021-22327 MISC
huawei -- multiple_smart_phones	There is an out of bounds write vulnerability in Huawei Smartphone HUAWEI P30 versions 9.1.0.131(C00E130R1P21) when processing a message. An unauthenticated attacker can exploit this vulnerability by sending specific message to the target device. Due to insufficient validation of the input parameter, successful exploit can cause the process and the service to be abnormal.	2021-04-28	not yet calculated	CVE-2021-22330 MISC
huawei -- multiple_smart_phones	There is a JavaScript injection vulnerability in certain Huawei smartphones. A module does not verify some inputs sufficiently. Attackers can exploit this vulnerability by sending a malicious application request to launch JavaScript injection. This may compromise normal service. Affected product versions include HUAWEI P30 versions earlier than 10.1.0.165(C01E165R2P11), 11.0.0.118(C635E2R1P3), 11.0.0.120(C00E120R2P5), 11.0.0.138(C10E4R5P3), 11.0.0.138(C185E4R7P3), 11.0.0.138(C432E8R2P3), 11.0.0.138(C461E4R3P3), 11.0.0.138(C605E4R1P3), and 11.0.0.138(C636E4R3P3).	2021-04-28	not yet calculated	CVE-2021-22331 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- content_navigator	IBM Content Navigator 3.0.CD is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199168.	2021-04-27	not yet calculated	CVE-2021-20550 XF CONFIRM
ibm -- content_navigator	IBM Content Navigator 3.0.CD is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199167.	2021-04-27	not yet calculated	CVE-2021-20549 CONFIRM XF
ibm -- content_navigator	IBM Content Navigator 3.0.CD is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 196624.	2021-04-27	not yet calculated	CVE-2021-20448 CONFIRM XF
ibm -- spectrum_scale	IBM Spectrum Scale 5.0.0 through 5.0.5.6 and 5.1.0 through 5.1.0.2 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 199403.	2021-04-27	not yet calculated	CVE-2021-29667 CONFIRM XF
ibm -- spectrum_scale	IBM Spectrum Scale 5.0.0 through 5.0.5.6 and 5.1.0 through 5.1.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199400.	2021-04-27	not yet calculated	CVE-2021-29666 XF CONFIRM
ibm -- spectrum_scale	IBM Spectrum Scale 5.0.4.1 through 5.1.0.3 could allow a local privileged user to overwrite files due to improper input validation. IBM X-Force ID: 192541.	2021-04-27	not yet calculated	CVE-2020-4981 CONFIRM XF
icms -- icms	Path Traversal in iCMS v7.0.13 allows remote attackers to delete folders by injecting commands into a crafted HTTP request to the "do_del()" method of the component "database.admincp.php".	2021-04-30	not yet calculated	CVE-2020-18070 MISC
inim -- electronics_smartliving_smart	Inim Electronics SmartLiving SmartLAN/G/SI <=6.x suffers from an authenticated remote command injection vulnerability. The issue exist due to the 'par' POST parameter not being sanitized when called with the 'testemail' module through web.cgi binary. The vulnerable CGI binary (ELF 32-bit LSB executable, ARM) is calling the 'sh' executable via the system() function to issue a command using the mailx service and its vulnerable string format parameter allowing for OS command injection with root privileges. An attacker can remotely execute system commands as the root user using default credentials and bypass access controls in place.	2021-04-29	not yet calculated	CVE-2020-21992 MISC
inim -- electronics_smartliving_smart	Inim Electronics Smartliving SmartLAN/G/SI <=6.x uses default hardcoded credentials. An attacker could exploit this to gain Telnet, SSH and FTP access to the system.	2021-04-29	not yet calculated	CVE-2020-21995 EXPLOIT-DB MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
inim -- electronics_smartliving_smart	An Unauthenticated Server-Side Request Forgery (SSRF) vulnerability exists in Inim Electronics Smartliving SmartLAN/G/SI <=6.x within the GetImage functionality. The application parses user supplied data in the GET parameter 'host' to construct an image request to the service through onvif.cgi. Since no validation is carried out on the parameter, an attacker can specify an external domain and force the application to make an HTTP request to an arbitrary destination host.	2021-04-29	not yet calculated	CVE-2020-22002 MISC MISC
jansson -- jansson	** DISPUTED ** An issue was discovered in Jansson through 2.13.1. Due to a parsing error in json_loads, there's an out-of-bounds read-access bug. NOTE: the vendor reports that this only occurs when a programmer fails to follow the API specification.	2021-04-26	not yet calculated	CVE-2020-36325 MISC
jeesns -- jeesns	Cross Site Scripting (XSS) in Jeesns v1.4.2 allows remote attackers to execute arbitrary code by injecting commands into the "CKEditorFuncNum" parameter in the component "CkeditorUploadController.java".	2021-04-29	not yet calculated	CVE-2020-18035 MISC
key_recovery_authority -- key_recovery_authority	A flaw was found in the Key Recovery Authority (KRA) Agent Service in pki-core 10.10.5 where it did not properly sanitize the recovery ID during a key recovery request, enabling a reflected cross-site scripting (XSS) vulnerability. An attacker could trick an authenticated victim into executing specially crafted Javascript code.	2021-04-30	not yet calculated	CVE-2020-1721 MISC
kilbc -- kilbc	An issue was discovered in klibc before 2.0.9. Multiple possible integer overflows in the cpio command on 32-bit systems may result in a buffer overflow or other security impact.	2021-04-30	not yet calculated	CVE-2021-31872 MISC MISC MISC MLIST
kilbc -- kilbc	An issue was discovered in klibc before 2.0.9. Multiplication in the calloc() function may result in an integer overflow and a subsequent heap buffer overflow.	2021-04-30	not yet calculated	CVE-2021-31870 MISC MISC MISC MLIST
kilbc -- kilbc	An issue was discovered in klibc before 2.0.9. An integer overflow in the cpio command may result in a NULL pointer dereference on 64-bit systems.	2021-04-30	not yet calculated	CVE-2021-31871 MISC MISC MISC MLIST
kilbc -- kilbc	An issue was discovered in klibc before 2.0.9. Additions in the malloc() function may result in an integer overflow and a subsequent heap buffer overflow.	2021-04-30	not yet calculated	CVE-2021-31873 MISC MISC MISC MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kirby -- kirby	Kirby is an open source CMS. An editor with write access to the Kirby Panel can upload an SVG file that contains harmful content like `<script>` tags. The direct link to that file can be sent to other users or visitors of the site. If the victim opens that link in a browser where they are logged in to Kirby, the script will run and can for example trigger requests to Kirby's API with the permissions of the victim. This vulnerability is critical if you might have potential attackers in your group of authenticated Panel users, as they can escalate their privileges if they get access to the Panel session of an admin user. Depending on your site, other JavaScript-powered attacks are possible. Visitors without Panel access can only use this attack vector if your site allows SVG file uploads in frontend forms and you don't already sanitize uploaded SVG files. The problem has been patched in Kirby 3.5.4. Please update to this or a later version to fix the vulnerability. Frontend upload forms need to be patched separately depending on how they store the uploaded file(s). If you use `File::create()`, you are protected by updating to 3.5.4+. As a work around you can disable the upload of SVG files in your file blueprints.	2021-04-27	not yet calculated	CVE-2021-29460 CONFIRM MISC MISC
lenovo -- pcmanager	A denial of service vulnerability was reported in Lenovo PCManager, prior to version 3.0.400.3252, that could allow configuration files to be written to non-standard locations.	2021-04-27	not yet calculated	CVE-2021-3451 MISC
lenovo -- pcmanager	A DLL search path vulnerability was reported in Lenovo PCManager, prior to version 3.0.400.3252, that could allow privilege escalation.	2021-04-27	not yet calculated	CVE-2021-3464 MISC
leocad -- leocad	LeoCAD before 21.03 sometimes allows a use-after-free during the opening of a new document.	2021-04-26	not yet calculated	CVE-2021-31804 MISC
libezxml -- ezxml	An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_decode() performs incorrect memory handling while parsing crafted XML files, leading to a heap-based buffer overflow.	2021-04-24	not yet calculated	CVE-2021-31598 MISC
libimage-exiftool-perl -- libimage-exiftool-perl	Improper neutralization of user data in the DjVu file format in ExifTool versions 7.44 and up allows arbitrary code execution when parsing the malicious image	2021-04-23	not yet calculated	CVE-2021-22204 MISC MISC CONFIRM DEBIAN
lilin -- ip_camera_device	The NTP Server configuration function of the IP camera device is not verified with special parameters. Remote attackers can perform a command Injection attack and execute arbitrary commands after logging in with the privileged permission.	2021-04-28	not yet calculated	CVE-2021-30166 MISC MISC MISC MISC
lilin -- webcam_device	The sensitive information of webcam device is not properly protected. Remote attackers can unauthentically grant user’s credential.	2021-04-28	not yet calculated	CVE-2021-30169 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	The PowerVR GPU kernel driver in pvrsrvkm.ko through 2021-04-24 for the Linux kernel, as used on Alcatel 1S phones, allows attackers to overwrite heap memory via PhysmemNewRamBackedPMR.	2021-04-24	not yet calculated	CVE-2021-31795 MISC
live555 -- streaming_media	Vulnerability in the AC3AudioFileServerMediaSubsession, ADTSAudioFileServerMediaSubsession, and AMRAudioFileServerMediaSubsessionLive OnDemandServerMediaSubsession subclasses in Networks LIVE555 Streaming Media before 2021.3.16.	2021-04-29	not yet calculated	CVE-2021-28899 MISC
managewiki -- managewiki	ManageWiki is an extension to the MediaWiki project. The 'wikiconfig' API leaked the value of private configuration variables set through the ManageWiki variable to all users. This has been patched by https://github.com/miraheze/ManageWiki/compare/99f3b228af18...[illegible].patch. If you are unable to patch set `$wgAPIListModules['wikiconfig'] = 'ApiQueryDisabled';` or remove private config as a workaround.	2021-04-28	not yet calculated	CVE-2021-29483 CONFIRM MISC MISC
md4c.c -- md4c.c	md_analyze_line in md4c.c in md4c 0.4.7 allows attackers to trigger use of uninitialized memory, and cause a denial of service via a malformed Markdown document.	2021-04-29	not yet calculated	CVE-2021-30027 MISC MISC
media2click -- media2click	The media2click (aka 2 Clicks for External Media) extension 1.x before 1.3.3 for TYPO3 allows XSS by a backend user account.	2021-04-28	not yet calculated	CVE-2021-31778 MISC
mercury -- mercury	MERCUSYS Mercury X18G 1.0.5 devices allow Denial of service via a crafted value to the POST listen_http_lan parameter. Upon subsequent device restarts after this vulnerability is exploted the device will not be able to access the webserver unless the listen_http_lan parameter to uhttpd.json is manually fixed.	2021-04-29	not yet calculated	CVE-2021-25811 MISC MISC MISC
mercury -- mercury	Cross site Scripting (XSS) vulnerability in MERCUSYS Mercury X18G 1.0.5 devices, via crafted values to the 'src_dport_start', 'src_dport_end', and 'dest_port' parameters.	2021-04-29	not yet calculated	CVE-2021-25810 MISC MISC MISC
meshery -- meshery	A SQL Injection vulnerability in the REST API in Layer5 Meshery 0.5.2 allows an attacker to execute arbitrary SQL commands via the /experimental/patternfiles endpoint (order parameter in GetMesheryPatterns in models/meshery_pattern_persister.go).	2021-04-28	not yet calculated	CVE-2021-31856 MISC MISC
micro_focus -- application_performance_management	An arbitrary code execution vulnerability exists in Micro Focus Application Performance Management, affecting versions 9.40, 9.50 and 9.51. The vulnerability could allow remote attackers to execute arbitrary code on affected installations of APM.	2021-04-28	not yet calculated	CVE-2021-22514 MISC
minicms -- minicms	Cross Site Scripting (XSS) in MiniCMS v1.10 allows remote attackers to execute arbitrary code by injecting commands via a crafted HTTP request to the component "/mc-admin/post-edit.php".	2021-04-28	not yet calculated	CVE-2020-17999 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
minthcm -- release	A weak password requirement vulnerability exists in the Create New User function of MintHCM RELEASE 3.0.8, which could lead an attacker to easier password brute-forcing.	2021-04-26	not yet calculated	CVE-2021-25839 MISC MISC
misp -- misp	In app/Model/MispObject.php in MISP 2.4.141, an incorrect sharing group association could lead to information disclosure on an event edit. When an object has a sharing group associated with an event edit, the sharing group object is ignored and instead the passed local ID is reused.	2021-04-23	not yet calculated	CVE-2021-31780 MISC
mongodb -- mongodb	A user authorized to performing a specific type of find query may trigger a denial of service. This issue affects: MongoDB Inc. MongoDB Server v4.4 versions prior to 4.4.4.	2021-04-30	not yet calculated	CVE-2021-20326 CONFIRM
nacos -- nacos	Nacos is a platform designed for dynamic service discovery and configuration and service management. In Nacos before version 1.4.1, the ConfigOpsController lets the user perform management operations like querying the database or even wiping it out. While the /data/remove endpoint is properly protected with the @Secured annotation, the /derby endpoint is not protected and can be openly accessed by unauthenticated users. These endpoints are only valid when using embedded storage (derby DB) so this issue should not affect those installations using external storage (e.g. mysql)	2021-04-27	not yet calculated	CVE-2021-29442 MISC MISC CONFIRM
nacos -- nacos	Nacos is a platform designed for dynamic service discovery and configuration and service management. In Nacos before version 1.4.1, when configured to use authentication (-Dnacos.core.auth.enabled=true) Nacos uses the AuthFilter servlet filter to enforce authentication. This filter has a backdoor that enables Nacos servers to bypass this filter and therefore skip authentication checks. This mechanism relies on the user-agent HTTP header so it can be easily spoofed. This issue may allow any user to carry out any administrative tasks on the Nacos server.	2021-04-27	not yet calculated	CVE-2021-29441 MISC CONFIRM MISC
nec -- aterm_devices	NEC Aterm devices (Aterm WF1200CR firmware Ver1.3.2 and earlier, Aterm WG1200CR firmware Ver1.3.3 and earlier, and Aterm WG2600HS firmware Ver1.5.1 and earlier) allow authenticated attackers to execute arbitrary OS commands by sending a specially crafted request to a specific URL.	2021-04-26	not yet calculated	CVE-2021-20708 MISC MISC
nec -- aterm_devices	Improper validation of integrity check value vulnerability in NEC Aterm WF1200CR firmware Ver1.3.2 and earlier, Aterm WG1200CR firmware Ver1.3.3 and earlier, and Aterm WG2600HS firmware Ver1.5.1 and earlier allows an attacker with an administrative privilege to execute arbitrary OS commands by sending a specially crafted request to a specific URL.	2021-04-26	not yet calculated	CVE-2021-20709 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nec -- aterm_devices	Cross-site scripting vulnerability in NEC Aterm devices (Aterm WG1900HP2 firmware Ver.1.3.1 and earlier, Aterm WG1900HP firmware Ver.2.5.1 and earlier, Aterm WG1800HP4 firmware Ver.1.3.1 and earlier, Aterm WG1800HP3 firmware Ver.1.5.1 and earlier, Aterm WG1200HS2 firmware Ver.2.5.0 and earlier, Aterm WG1200HP3 firmware Ver.1.3.1 and earlier, Aterm WG1200HP2 firmware Ver.2.5.0 and earlier, Aterm W1200EX firmware Ver.1.3.1 and earlier, Aterm W1200EX-MS firmware Ver.1.3.1 and earlier, Aterm WG1200HS firmware all versions Aterm WG1200HP firmware all versions Aterm WF800HP firmware all versions Aterm WF300HP2 firmware all versions Aterm WR8165N firmware all versions Aterm W500P firmware all versions, and Aterm W300P firmware all versions) allows remote attackers to inject arbitrary script or HTML via unspecified vectors.	2021-04-26	not yet calculated	CVE-2021-20680 MISC MISC
nec -- aterm_devices	Improper access control vulnerability in NEC Aterm WG2600HS firmware Ver1.5.1 and earlier, and Aterm WX3000HP firmware Ver1.1.2 and earlier allows a device connected to the LAN side to be accessed from the WAN side due to the defect in the IPv6 firewall function.	2021-04-26	not yet calculated	CVE-2021-20712 MISC MISC
netgear -- r7000_devices	NETGEAR R7000 1.0.11.116 devices have a heap-based Buffer Overflow that is exploitable from the local network without authentication. The vulnerability exists within the handling of an HTTP request. An attacker can leverage this to execute code as root. The problem is that a user-provided length value is trusted during a backup.cgi file upload. The attacker must add a \n before the Content-Length header.	2021-04-26	not yet calculated	CVE-2021-31802 MISC MISC
npupnp -- npupnp	The server in npupnp before 4.1.4 is affected by DNS rebinding in the embedded web server (including UPnP SOAP and GENA endpoints), leading to remote code execution.	2021-04-25	not yet calculated	CVE-2021-31718 MISC MISC MISC
nvidia -- virtual_gpu_manager	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), in which an input length is not validated, which may lead to information disclosure, tampering of data, or denial of service. vGPU version 12.x (prior to 12.2), version 11.x (prior to 11.4) and version 8.x (prior to 8.7)	2021-04-29	not yet calculated	CVE-2021-1082 CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA vGPU driver contains a vulnerability in the guest kernel mode driver and Virtual GPU Manager (vGPU plugin), in which an input length is not validated, which may lead to tampering of data or denial of service. This affects vGPU version 12.x (prior to 12.2) and version 11.x (prior to 11.4).	2021-04-29	not yet calculated	CVE-2021-1084 CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA vGPU driver contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where there is the potential to write to a shared memory location and manipulate the data after the data has been validated, which may lead to denial of service and escalation of privileges. This affects vGPU version 12.x (prior to 12.2), version 11.x (prior to 11.4) and version 8.x (prior to 8.7).	2021-04-29	not yet calculated	CVE-2021-1085 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nvidia -- virtual_gpu_manager	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and Virtual GPU Manager (vGPU plugin), in which an input length is not validated, which may lead to information disclosure, tampering of data, or denial of service. This affects vGPU version 12.x (prior to 12.2) and version 11.x (prior to 11.4).	2021-04-29	not yet calculated	CVE-2021-1083 CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA vGPU driver contains a vulnerability in the Virtual GPU Manager (vGPU plugin), which could allow an attacker to retrieve information that could lead to a Address Space Layout Randomization (ASLR) bypass. This affects vGPU version 12.x (prior to 12.2), version 11.x (prior to 11.4) and version 8.x (prior to 8.7).	2021-04-29	not yet calculated	CVE-2021-1087 CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA vGPU software contains a vulnerability in the guest kernel mode driver and Virtual GPU manager (vGPU plugin), in which an input length is not validated, which may lead to information disclosure, tampering of data, or denial of service. This affects vGPU version 12.x (prior to 12.2), version 11.x (prior to 11.4) and version 8.x (prior 8.7).	2021-04-29	not yet calculated	CVE-2021-1081 CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), in which certain input data is not validated, which may lead to information disclosure, tampering of data, or denial of service. This affects vGPU version 12.x (prior to 12.2), version 11.x (prior to 11.4) and version 8.x (prior 8.7).	2021-04-29	not yet calculated	CVE-2021-1080 CONFIRM
nvidia -- virtual_gpu_manager	NVIDIA vGPU driver contains a vulnerability in the Virtual GPU Manager (vGPU plugin) where it allows guests to control unauthorized resources, which may lead to integrity and confidentiality loss or information disclosure. This affects vGPU version 12.x (prior to 12.2), version 11.x (prior to 11.4) and version 8.x (prior to 8.7).	2021-04-29	not yet calculated	CVE-2021-1086 CONFIRM
open_design_alliance -- sdk	An out-of-bounds write vulnerability exists in the file-reading procedure in Open Design Alliance Drawings SDK before 2021.6 on all supported by ODA platforms in static configuration. This can allow attackers to cause a crash, potentially enabling a denial of service attack (Crash, Exit, or Restart) or possible code execution.	2021-04-26	not yet calculated	CVE-2021-31784 MISC
openapi -- generator	OpenAPI Generator allows generation of API client libraries, server stubs, documentation and configuration automatically given an OpenAPI Spec. Using `File.createTempFile` in JDK will result in creating and using insecure temporary files that can leave application and system data vulnerable to attacks. OpenAPI Generator maven plug-in creates insecure temporary files during the process. The issue has been patched with `Files.createTempFile` and released in the v5.1.0 stable version.	2021-04-27	not yet calculated	CVE-2021-21429 MISC CONFIRM
openvpn -- openvpn	OpenVPN 2.5.1 and earlier versions allows a remote attackers to bypass authentication and access control channel data on servers configured with deferred authentication, which can be used to potentially trigger further information leaks.	2021-04-26	not yet calculated	CVE-2020-15078 MISC MISC FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is Prior to 6.1.20. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	2021-04-28	not yet calculated	CVE-2021-2321 MISC
orangehrm -- orangehrm	OrangeHRM 4.7 allows an unauthenticated user to enumerate the valid username and email address via the forgot password function.	2021-04-26	not yet calculated	CVE-2021-28399 MISC MISC
ox -- app_suite	OX App Suite 7.10.4 and earlier allows SSRF via a snippet.	2021-04-30	not yet calculated	CVE-2020-28943 MISC MISC
ox -- app_suite	OX App Suite 7.10.4 and earlier allows XSS via a crafted contact object (payload in the position or company field) that is mishandled in the App Suite UI on a smartphone.	2021-04-30	not yet calculated	CVE-2021-31934 MISC
ox -- app_suite	OX App Suite 7.10.4 and earlier allows XSS via a crafted distribution list (payload in the common name) that is mishandled in the scheduling view.	2021-04-30	not yet calculated	CVE-2021-31935 MISC
ox -- guard	OX Guard 2.10.4 and earlier allows a Denial of Service via a WKS server that responds slowly or with a large amount of data.	2021-04-30	not yet calculated	CVE-2020-28944 MISC MISC
parallels -- desktop	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.5-47309. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12528.	2021-04-29	not yet calculated	CVE-2021-31423 MISC MISC
parallels -- desktop	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.4-47270. An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12221.	2021-04-29	not yet calculated	CVE-2021-31418 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
parallels -- desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.0-48950. An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12220.	2021-04-29	not yet calculated	CVE-2021-31420 MISC MISC
parallels -- desktop	This vulnerability allows local attackers to delete arbitrary files on affected installations of Parallels Desktop 16.1.1-49141. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to delete arbitrary files in the context of the hypervisor. Was ZDI-CAN-12129.	2021-04-29	not yet calculated	CVE-2021-31421 MISC MISC
parallels -- desktop	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.5-47309. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the IDE virtual device. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13190.	2021-04-29	not yet calculated	CVE-2021-31432 MISC MISC
parallels -- desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.5-47309. An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Open Tools Gate component. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12848.	2021-04-29	not yet calculated	CVE-2021-31424 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
parallels -- desktop	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.5-47309. An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Open Tools Gate component. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13082.	2021-04-29	not yet calculated	CVE-2021-31427 MISC MISC
parallels -- desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.5-47309. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the IDE virtual device. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13186.	2021-04-29	not yet calculated	CVE-2021-31428 MISC MISC
parallels -- desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 15.1.5-47309. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the IDE virtual device. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13187.	2021-04-29	not yet calculated	CVE-2021-31429 MISC MISC
parallels -- desktop	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.5-47309. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the IDE virtual device. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13189.	2021-04-29	not yet calculated	CVE-2021-31431 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
parallels -- desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.2-49151. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Parallels Tools component. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the kernel on the target guest system. Was ZDI-CAN-12791.	2021-04-29	not yet calculated	CVE-2021-31426 MISC MISC
parallels -- desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.2-49151. An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Parallels Tools component. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the kernel on the target guest system. Was ZDI-CAN-12790.	2021-04-29	not yet calculated	CVE-2021-31425 MISC MISC
parallels -- desktop	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.1.1-49141. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the e1000e virtual device. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12527.	2021-04-29	not yet calculated	CVE-2021-31422 MISC MISC
parallels -- desktop	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.4-47270. An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12131.	2021-04-29	not yet calculated	CVE-2021-31417 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
parallels -- desktop	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.5-47309. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the IDE virtual device. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-13188.	2021-04-29	not yet calculated	CVE-2021-31430 MISC MISC
parallels -- desktop	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 15.1.4-47270. An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12136.	2021-04-29	not yet calculated	CVE-2021-31419 MISC MISC
pdfresurrect -- pdfresurrect	A flaw was found in PDFResurrect in version 0.22b. There is an infinite loop in get_xref_linear_skipped() in pdf.c via a crafted PDF file.	2021-04-28	not yet calculated	CVE-2021-3508 MISC MISC
pega -- infinity	In versions 8.2.1 through 8.5.2 of Pega Infinity, the password reset functionality for local accounts can be used to bypass local authentication checks.	2021-04-29	not yet calculated	CVE-2021-27651 CONFIRM
pgsync -- pgsync	pgsync before 0.6.7 is affected by Information Disclosure of sensitive information. Syncing the schema with the --schema-first and --schema-only options is mishandled. For example, the sslmode connection parameter may be lost, which means that SSL would not be used.	2021-04-27	not yet calculated	CVE-2021-31671 MISC
phpfusion -- phpfusion	CSRF + Cross-site scripting (XSS) vulnerability in search.php in PHPFusion 9.03.110 allows remote attackers to inject arbitrary web script or HTML	2021-04-29	not yet calculated	CVE-2021-28280 MISC MISC MISC MISC MISC
phpmailer -- phpmailer	PHPMailer 6.1.8 through 6.4.0 allows object injection through Phar Deserialization via addAttachment with a UNC pathname. NOTE: this is similar to CVE-2018-19296, but arose because 6.1.8 fixed a functionality problem in which UNC pathnames were always considered unreadable by PHPMailer, even in safe contexts. As an unintended side effect, this fix eliminated the code that blocked addAttachment exploitation.	2021-04-28	not yet calculated	CVE-2020-36326 MISC
phpshe -- mall_system	SQL Injection in PHPSHE Mall System v1.7 allows remote attackers to execute arbitrary code by injecting SQL commands into the "user_phone" parameter of a crafted HTTP request to the "admin.php" component.	2021-04-28	not yet calculated	CVE-2020-18020 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
piwigo -- piwigo	show_default.php in the LocalFilesEditor extension before 11.4.0.1 for Piwigo allows Local File Inclusion because the file parameter is not validated with a proper regular-expression check.	2021-04-26	not yet calculated	CVE-2021-31783 MISC MISC MISC
postcss -- postcss	The package postcss before 8.2.13 are vulnerable to Regular Expression Denial of Service (ReDoS) via getAnnotationURL() and loadAnnotation() in lib/previous-map.js. The vulnerable regexes are caused mainly by the sub-pattern \/*\s* sourceMappingURL=(.*).	2021-04-26	not yet calculated	CVE-2021-23382 MISC MISC MISC
prisma -- prisma	Prisma is an open source ORM for Node.js & TypeScript. As of today, we are not aware of any Prisma users or external consumers of the `@prisma/sdk` package who are affected by this security vulnerability. This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input. It only affects the `getPackedPackage` function and this function is not advertised and only used for tests & building our CLI, no malicious code was found after checking our codebase.	2021-04-29	not yet calculated	CVE-2021-21414 MISC CONFIRM
prisma -- vs_code	Prisma VS Code a VSCode extension for Prisma schema files. This is a Remote Code Execution Vulnerability that affects all versions of the Prisma VS Code extension older than 2.20.0. If a custom binary path for the Prisma format binary is set in VS Code Settings, for example by downloading a project that has a .vscode/settings.json file that sets a value for "prismaFmtBinPath". That custom binary is executed when auto-formatting is triggered by VS Code or when validation checks are triggered after each keypress on a *.prisma file. Fixed in versions 2.20.0 and 20.0.27. As a workaround users can either edit or delete the `.vscode/settings.json` file or check if the binary is malicious and delete it.	2021-04-29	not yet calculated	CVE-2021-21415 MISC MISC CONFIRM MISC
pritunl -- client	Pritunl Client v1.2.2550.20 contains a local privilege escalation vulnerability in the pritunl-service component. The attack vector is: malicious openvpn config. A local attacker could leverage the log and log-append along with log injection to create or append to privileged script files and execute code as root/SYSTEM.	2021-04-30	not yet calculated	CVE-2020-27519 MISC MISC CONFIRM
qibsoft -- qibocms	Cross Site Scripting (XSS) in Qibosoft QiboCMS v7 and earlier allows remote attackers to execute arbitrary code or obtain sensitive information by injecting arbitrary commands in a HTTP request to the "ewebeditor.1.1\kindeditor.js" component.	2021-04-28	not yet calculated	CVE-2020-18022 MISC
react-draft-wysiwyg -- react-draft-wysiwyg	react-draft-wysiwyg (aka React Draft Wysiwyg) before 1.14.6 allows a javascript: URi in a Link Target of the link decorator in decorators/Link/index.js when a draft is shared across users, leading to XSS.	2021-04-24	not yet calculated	CVE-2021-31712 MISC MISC CONFIRM
redmine -- redmine	Redmine before 4.0.9, 4.1.x before 4.1.3, and 4.2.x before 4.2.1 allows users to circumvent the allowed filename extensions of uploaded attachments.	2021-04-28	not yet calculated	CVE-2021-31865 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
redmine -- redmine 	Redmine before 4.0.9, 4.1.x before 4.1.3, and 4.2.x before 4.2.1 allows attackers to bypass the add_issue_notes permission requirement by leveraging the incoming mail handler.	2021-04-28	not yet calculated	CVE-2021-31864 MISC MISC
redmine -- redmine 	Redmine before 4.0.9 and 4.1.x before 4.1.3 allows an attacker to learn the values of internal authentication keys by observing timing differences in string comparison operations within SysController and MailHandlerController.	2021-04-28	not yet calculated	CVE-2021-31866 MISC MISC
redmine -- redmine 	Insufficient input validation in the Git repository integration of Redmine before 4.0.9, 4.1.x before 4.1.3, and 4.2.x before 4.2.1 allows Redmine users to read arbitrary local files accessible by the application server process.	2021-04-28	not yet calculated	CVE-2021-31863 MISC MISC
rukovoditel -- rukovoditel 	Cross Site Request Forgery (CSRF) in Rukovoditel v2.8.3 allows attackers to create an admin user with an arbitrary credentials.	2021-04-29	not yet calculated	CVE-2021-30224 MISC MISC
russelhaering -- gosaml2 	This affects all versions of package github.com/russellhaering/gosaml2. There is a crash on nil-pointer dereference caused by sending malformed XML signatures.	2021-04-30	not yet calculated	CVE-2020-7731 CONFIRM CONFIRM
rust -- rkyv 	An issue was discovered in the rkyv crate before 0.6.0 for Rust. When an archive is created via serialization, the archive content may contain uninitialized values of certain parts of a struct.	2021-04-30	not yet calculated	CVE-2021-31919 MISC
safe-flat -- safe-flat 	Prototype pollution vulnerability in 'safe-flat' versions 2.0.0 through 2.0.1 allows an attacker to cause a denial of service and may lead to remote code execution.	2021-04-26	not yet calculated	CVE-2021-25927 MISC MISC
saltstack -- salt 	In SaltStack Salt 2016.9 through 3002.6, a command injection vulnerability exists in the snapper module that allows for local privilege escalation on a minion. The attack requires that a file is created with a pathname that is backed up by snapper, and that the master calls the snapper.diff function (which executes popen unsafely).	2021-04-23	not yet calculated	CVE-2021-31607 MISC FEDORA
samurai -- samurai 	samurai 1.2 has a NULL pointer dereference in writefile() in util.c via a crafted build file.	2021-04-29	not yet calculated	CVE-2021-30218 MISC MISC
samurai -- samurai 	samurai 1.2 has a NULL pointer dereference in printstatus() function in build.c via a crafted build file.	2021-04-29	not yet calculated	CVE-2021-30219 MISC MISC
screenly -- screenly-ose 	Cross Site Scriptiong vulnerabilityin Screenly screenly-ose all versions, including v1.8.2 (2019-09-25-Screenly-OSE-lite.img), in the 'Add Asset' page via manipulation of a 'URL' field, which could let a remote malicious user execute arbitrary code.	2021-04-29	not yet calculated	CVE-2020-21101 MISC
shibboleth -- service_provider 	Shibboleth Service Provider 3.x before 3.2.2 is prone to a NULL pointer dereference flaw involving the session recovery feature. The flaw is exploitable (for a daemon crash) on systems not using this feature if a crafted cookie is supplied.	2021-04-27	not yet calculated	CVE-2021-31826 MISC MISC MISC MISC DEBIAN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sipwise -- c5_ngcp	Sipwise C5 NGCP CSC through CE_m39.3.1 allows call/click2dial CSRF attacks for actions with administrative privileges	2021-04-23	not yet calculated	CVE-2021-31584 MISC MISC MISC
sipwise -- c5_ngcp	Sipwise C5 NGCP CSC through CE_m39.3.1 has multiple authenticated stored and reflected XSS vulnerabilities when input passed via several parameters to several scripts is not properly sanitized before being returned to the user: Stored XSS in callforward/time/set/save (POST tsetname); Reflected XSS in addressbook (GET filter); Stored XSS in addressbook/save (POST firstname, lastname, company); and Reflected XSS in statistics/versions (GET lang).	2021-04-23	not yet calculated	CVE-2021-31583 MISC MISC MISC
smartwares -- home	Smartwares HOME easy <=1.0.9 is vulnerable to an unauthenticated database backup download and information disclosure vulnerability. An attacker could disclose sensitive and clear-text information resulting in authentication bypass, session hijacking and full system control.	2021-04-29	not yet calculated	CVE-2020-21997 MISC EXPLOIT-DB
sonatype -- nexus_repository_manager	Sonatype Nexus Repository Manager 3.x before 3.30.1 allows a remote attacker to get a list of files and directories that exist in a UI-related folder via directory traversal (no customer-specific data is exposed).	2021-04-27	not yet calculated	CVE-2021-30635 MISC
sonatype -- nexus_repository_manager_3	A cross-site scripting (XSS) vulnerability has been discovered in Nexus Repository Manager 3.x before 3.30.1. An attacker with a local account can create entities with crafted properties that, when viewed by an administrator, can execute arbitrary JavaScript in the context of the NXRM application.	2021-04-28	not yet calculated	CVE-2021-29159 MISC MISC
sonatype -- nexus_repository_manager_3_pro	Sonatype Nexus Repository Manager 3 Pro up to and including 3.30.0 has Incorrect Access Control.	2021-04-23	not yet calculated	CVE-2021-29158 MISC CONFIRM
sourcecodester -- budget_management_system	A stored cross-site scripting (XSS) vulnerability in SourceCodester Budget Management System 1.0 allows users to inject and store arbitrary JavaScript code in index.php via vulnerable field 'Budget Title'.	2021-04-28	not yet calculated	CVE-2021-29388 MISC MISC
sourcecodester -- equiptment_inventory_system	Multiple stored cross-site scripting (XSS) vulnerabilities in Sourcecodester Equipment Inventory System 1.0 allow remote attackers to inject arbitrary javascript via any "Add" sections, such as Add Item , Employee and Position or others in the Name Parameters.	2021-04-28	not yet calculated	CVE-2021-29387 MISC MISC
soyal_technology -- 701client	Soyal Technology 701Client 9.0.1 is vulnerable to Insecure permissions via client.exe binary with Authenticated Users group with Full permissions.	2021-04-27	not yet calculated	CVE-2021-28269 MISC MISC EXPLOIT-DB
soyal_technology -- 701server	Soyal Technologies SOYAL 701Server 9.0.1 suffers from an elevation of privileges vulnerability which can be used by an authenticated user to change the executable file with a binary choice. The vulnerability is due to improper permissions with the 'F' flag (Full) for 'Everyone'and 'Authenticated Users' group.	2021-04-27	not yet calculated	CVE-2021-28271 EXPLOIT-DB MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
suitecrm -- suitecrm	XSS in the client account page in SuiteCRM before 7.11.19 allows an attacker to inject JavaScript via the name field	2021-04-30	not yet calculated	CVE-2021-31792 MISC MISC MISC
susi -- ai_server	SUSI.AI is an intelligent Open Source personal assistant. SUSI.AI Server before version d27ed0f has a directory traversal vulnerability due to insufficient input validation. Any admin config and file readable by the app can be retrieved by the attacker. Furthermore, some files can also be moved or deleted.	2021-04-30	not yet calculated	CVE-2020-4039 CONFIRM
symantec -- security_analytics_web	An input validation flaw in the Symantec Security Analytics web UI 7.2 prior 7.2.7, 8.1, prior to 8.1.3-NSR3, 8.2, prior to 8.2.1-NSR2 or 8.2.2 allows a remote, unauthenticated attacker to execute arbitrary OS commands on the target with elevated privileges.	2021-04-27	not yet calculated	CVE-2021-30642 MISC
synology -- antivirus_essential	Externally controlled reference to a resource in another sphere in quarantine functionality in Synology Antivirus Essential before 1.4.8-2801 allows remote authenticated users to obtain privilege via unspecified vectors.	2021-04-28	not yet calculated	CVE-2021-27648 CONFIRM
systeminformation -- systeminformation	systeminformation is an open source system and OS information library for node.js. A command injection vulnerability has been discovered in versions of systeminformation prior to 5.6.4. The issue has been fixed with a parameter check on user input. Please upgrade to version >= 5.6.4. If you cannot upgrade, be sure to check or sanitize service parameters that are passed to si.inetLatency(), si.inetChecksite(), si.services(), si.processLoad() and other commands. Only allow strings, reject any arrays. String sanitation works as expected.	2021-04-29	not yet calculated	CVE-2021-21388 MISC MISC MISC CONFIRM MISC
tyk-identity-broker -- tyk-identity-broker	The package github.com/tyktechnologies/tyk-identity-broker before 1.1.1 are vulnerable to Authentication Bypass via the Go XML parser which can cause SAML authentication bypass. This is because the XML parser doesn't guarantee integrity in the XML round-trip (encoding/decoding XML data).	2021-04-26	not yet calculated	CVE-2021-23365 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
typo3 -- bootstrap_package	Bootstrap Package is a theme for TYPO3. It has been discovered that rendering content in the website frontend is vulnerable to cross-site scripting. A valid backend user account is needed to exploit this vulnerability. Users of the extension, who have overwritten the affected templates with custom code must manually apply the security fix. Update to version 7.1.2, 8.0.8, 9.1.4, 10.0.10 or 11.0.3 of the Bootstrap Package that fix the problem described. Updated version are available from the TYPO3 extension manager, Packagist and at https://extensions.typo3.org/extension/download/bootstrap_package/.	2021-04-27	not yet calculated	CVE-2021-21365 MISC CONFIRM MISC
typo3 -- dynamic_content_element	The dce (aka Dynamic Content Element) extension 2.2.0 through 2.6.x before 2.6.2, and 2.7.x before 2.7.1, for TYPO3 allows SQL Injection via a backend user account.	2021-04-28	not yet calculated	CVE-2021-31777 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
unisys -- data_exchange_management_studio	Unisys Data Exchange Management Studio through 5.0.34 doesn't sanitize the input to a HTML document field. This could be used for an XSS attack.	2021-04-27	not yet calculated	CVE-2020-35542 MISC
uniview -- uniview	An issue was discovered in uniview ISC2500-S. This is an upload vulnerability where an attacker can upload malicious code via /Interface/DevManage/EC.php?cmd=upload	2021-04-29	not yet calculated	CVE-2020-21452 MISC
void -- aural_rec_monitor	An issue was discovered in svc-login.php in Void Aural Rec Monitor 9.0.0.1. Passwords are stored in unencrypted source-code text files. This was noted when accessing the svc-login.php file. The value is used to authenticate a high-privileged user upon authenticating with the server.	2021-04-23	not yet calculated	CVE-2021-25898 MISC MISC
void -- aural_rec_monitor	An issue was discovered in svc-login.php in Void Aural Rec Monitor 9.0.0.1. An unauthenticated attacker can send a crafted HTTP request to perform a blind time-based SQL Injection. The vulnerable parameter is param1.	2021-04-23	not yet calculated	CVE-2021-25899 MISC MISC
vtiger -- crm	An issue was dicovered in vtiger crm 7.2. Union sql injection in the calendar exportdata feature.	2021-04-29	not yet calculated	CVE-2020-22807 MISC
webaccess/scada -- webaccess/scada	Incorrect permissions are set to default on the ‘Project Management’ page of WebAccess/SCADA portal of WebAccess/SCADA Versions 9.0.1 and prior, which may allow a low-privileged user to update an administrator’s password and login as an administrator to escalate privileges on the system.	2021-04-26	not yet calculated	CVE-2021-22669 MISC
wems -- limited_enterprise_manager	In WEMS Limited Enterprise Manager 2.58, input passed to the GET parameter 'email' is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML code in a user's browser session in context of an affected site.	2021-04-28	not yet calculated	CVE-2020-21993 MISC MISC
wp -- fastest_cache	Directory traversal vulnerability in WP Fastest Cache versions prior to 0.9.1.7 allows a remote attacker with administrator privileges to delete arbitrary files on the server via unspecified vectors.	2021-04-27	not yet calculated	CVE-2021-20714 MISC MISC MISC
xinhu -- xinhu	SQL Injection in Xinhu OA System v1.8.3 allows remote attackers to obtain sensitive information by injecting arbitrary commands into the "typeid" variable of the "createfolderAjax" function in the "mode_worcAction.php" component.	2021-04-28	not yet calculated	CVE-2020-18019 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xorg-x11-server -- xorg-x11-server	A flaw was found in xorg-x11-server in versions before 1.20.11. An integer underflow can occur in xserver which can lead to a local privilege escalation. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-04-26	not yet calculated	CVE-2021-3472 MISC MISC MISC MISC DEBIAN MISC MLIST FEDORA FEDORA MLIST FEDORA FEDORA MISC GENTOO
xz -- xz	xz is a compression and decompression library focusing on the xz format completely written in Go. The function readUvarint used to read the xz container format may not terminate a loop provide malicous input. The problem has been fixed in release v0.5.8. As a workaround users can limit the size of the compressed file input to a reasonable size for their use case. The standard library had recently the same issue and got the CVE-2020-16845 allocated.	2021-04-28	not yet calculated	CVE-2021-29482 CONFIRM MISC
yii2_fecshop -- N/A	An issue was found in yii2_fecshop 2.x. There is a reflected XSS vulnerability in the check cart page.	2021-04-29	not yet calculated	CVE-2020-22808 CONFIRM MISC
yoast_seo -- yoast_seo	The yoast_seo (aka Yoast SEO) extension before 7.2.1 for TYPO3 allows SSRF via a backend user account.	2021-04-28	not yet calculated	CVE-2021-31779 MISC
yzmcms -- yzmcms	Cross Site Scripting (XSS) in yzmCMS v5.2 allows remote attackers to execute arbitrary code by injecting commands into the "referer" field of a POST request to the component "/member/index/login.html" when logging in.	2021-04-30	not yet calculated	CVE-2020-18084 MISC
zoho -- manageengine_eventlog_analyzer	Zoho ManageEngine Eventlog Analyzer through 12147 is vulnerable to unauthenticated directory traversal via an entry in a ZIP archive. This leads to remote code execution.	2021-04-30	not yet calculated	CVE-2021-28959 MISC MISC

Back to top

Share Bulletin

Powered by

GOVDELIVERY